

- **Board Type**
  - **FPGA Version**
3. Systematically ensure that you can retrieve this data (from a database, for example) when you later prepare to deploy the SM to subscriber premises.
  4. Return you to the Remote Subscribers tab of the AP.
  5. Click the link of the next SM that you wish to test.
  6. Repeat the test procedure from that point. When you have tested all of the SMs that you intend to test, return your browser to the General Status tab of the AP.

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

### 16.3.8 General Status Tab of the AP

An example of an AP General Status tab is displayed in [Figure 61](#).

The screenshot shows a web browser window titled 'General Status [root] - Microsoft Internet Explorer'. The address bar is empty. The page has a navigation menu on the left with links: Home, Configuration, Statistics, Tools, Account, Quick Start, Copyright, and Logoff. Below the menu, it says 'Account: root' and 'Level: ADMINISTRATOR'. The main content area has tabs for 'General Status', 'Session Status', 'Remote Subscribers', 'Event Log', and 'Network Interface'. The 'General Status' tab is active, showing the following information:

**Home => General Status**  
2.4GHz - Access Point - 0a-00-3e-20-a5-36

Device Information	
Device Type :	2.4GHz - Access Point - 0a-00-3e-20-a5-36
Software Version :	CANOPY 8.0 (Build 19) Mar 17 2006 16:46:09 AP-DES
Software BOOT Version :	CANOPYBOOT 3.0
Board Type :	P9
FPGA Version :	022705H
Uptime :	12d, 20:59:59
System Time :	12:29:46 03/01/2003
Last NTP Time Update :	00:00:00 00/00/0000
Ethernet Interface :	100Base-TX Full Duplex

Access Point Stats	
Registered SM Count :	4
GPS Sync Pulse Status :	Generating Sync

Site Information	
Site Name :	2.4 DES AP test
Site Contact :	JP
Site Location :	BOST AP Table

Key Features Information	
Scheduling Type :	Hardware
MP Double Rate :	Enable

At the bottom of the browser window, it says 'Logged in as root'.

**Figure 61: General Status tab of AP, example**

The General Status tab provides information on the operation of this AP. This is the tab that opens by default when you access the GUI of the AP. The General Status tab provides the following read-only fields.

**Device Type**

This field indicates the type of the Canopy module. Values include the frequency band of the AP, its module type, and its MAC address.

**Software Version**

This field indicates the Canopy system release, the time and date of the release, and whether communications involving the module are secured by DES or AES encryption (see [Encrypting Canopy Radio Transmissions](#) on Page 369). If you request technical support, provide the information from this field.

**Software BOOT Version**

This field indicates the version of the CANOPYBOOT file. If you request technical support, provide the information from this field.

**Board Type**

This field indicates the series of hardware. See [Designations for Hardware in Radios](#) on Page 365.

**FPGA Version**

This field indicates the version of the field-programmable gate array (FPGA) on the module. When you request technical support, provide the information from this field.

**Uptime**

This field indicates how long the module has operated since power was applied.

**System Time**

This field provides the current time. If the AP is connected to a CMM, then this field provides GMT (Greenwich Mean Time). Any SM that registers to the AP inherits the system time.

**Last NTP Time Update**

This field displays when the AP last used time sent from an NTP server. If the AP has not been configured in the Time tab of the Configuration page to request time from an NTP server, then this field is populated by 00:00:00 00/00/00.

**Ethernet Interface**

This field indicates the speed and duplex state of the Ethernet interface to the AP.

**Registered SM Count**

This field indicates how many SMs are registered to the AP.

**GPS Sync Pulse Status**

This field indicates the status of synchronization as follows:

- **Generating sync** indicates that the module is set to *generate* the sync pulse.
- **Receiving Sync** indicates that the module is set to *receive* a sync pulse from an outside source and is receiving the pulse.
- **ERROR: No Sync Pulse** indicates that the module is set to *receive* a sync pulse from an outside source and is not receiving the pulse.



**NOTE:**

When this message is displayed, the AP transmitter is turned off to avoid self-interference within the Canopy system.

**Site Name**

This field indicates the name of the physical module. You can assign or change this name in the SNMP tab of the AP Configuration page. This information is also set into the *sysName* SNMP MIB-II object and can be polled by an SNMP management server.

**Site Contact**

This field indicates contact information for the physical module. You can provide or change this information in the SNMP tab of the AP Configuration page. This information is also set into the *sysName* SNMP MIB-II object and can be polled by an SNMP management server.

**Site Location**

This field indicates site information for the physical module. You can provide or change this information in the SNMP tab of the AP Configuration page.

**Scheduling Type**

This field indicates the type of frame scheduler that is active in the AP.

**MP Double Rate**

This field indicates whether 2X modulation rate is enabled for the sector.

**16.3.9 Concluding the Test of Point-to-Multipoint Links**

To conclude the test, perform the following steps.

**Procedure 11: Verifying and recording information from the AP**

1. Confirm that the **GPS Sync Pulse Status** field indicates **Generating Sync**.  
*NOTE:* This indication confirms that the AP is properly functional.
2. While your browser is directed to this General Status tab, note (or print) the values of the following fields:
  - **Device type**
  - **Software Version**
  - **Software BOOT Version**
  - **Board Type**
  - **FPGA Version**
3. Systematically ensure that you can retrieve this data when you prepare to deploy the AP.

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

## 16.4 CONFIGURING A POINT-TO-POINT LINK FOR TEST



**NOTE:**

This section supports the Canopy 10- and 20-Mbps Backhaul Modules. To find setup and configuration guides that support the OFDM Series Backhaul Modules, refer to [Products Not Covered by This User Guide](#) on Page 34.

Perform the following steps to begin the test setup.

**Procedure 12: Setting up the BH for Quick Start**

1. In one hand, securely hold the top (larger shell) of the BH that you intend to deploy as a timing master. With the other hand, depress the lever in the back of the base cover (smaller shell). Remove the base cover.
2. Plug one end of a CAT 5 Ethernet cable into the timing master.
3. Plug the other end of the Ethernet cable into the jack in the pig tail that hangs from the power supply.
4. Plug the other connector of the pig tail into the Ethernet jack of the computing device.



**WARNING!**

From this point until you remove power from the BH, stay at least as far from the BH as the minimum separation distance specified in [Table 37](#) on Page 169.

5. Plug the power supply into an electrical outlet.
6. Power up the computing device.
7. Start the browser in the computing device.

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

The Canopy BH interface provides a series of web pages to configure and monitor the unit. These screens are subject to change by subsequent software releases.

You can access the web-based interface through only a computing device that is either directly connected or connected through a network to the BH. If the computing device is not connected to a network when you are configuring the module in your test environment, and if the computer has used a proxy server address and port to configure a Canopy module, then you may need to first disable the proxy setting in the computer.

To toggle the computer to *not* use the proxy setting, perform [Procedure 6](#) on Page 185.

In the address bar of your browser, enter the IP address of the BHM (default is 169.254.1.1). The BHM responds by opening the General Status tab of its Home page.

### 16.4.1 Quick Start Page of the BHM

To proceed with the test setup, click the **Quick Start** button on the left side of the General Status tab. The BHM responds by opening the Quick Start tab of the Quick Start page. An example of this tab is displayed in [Figure 62](#).

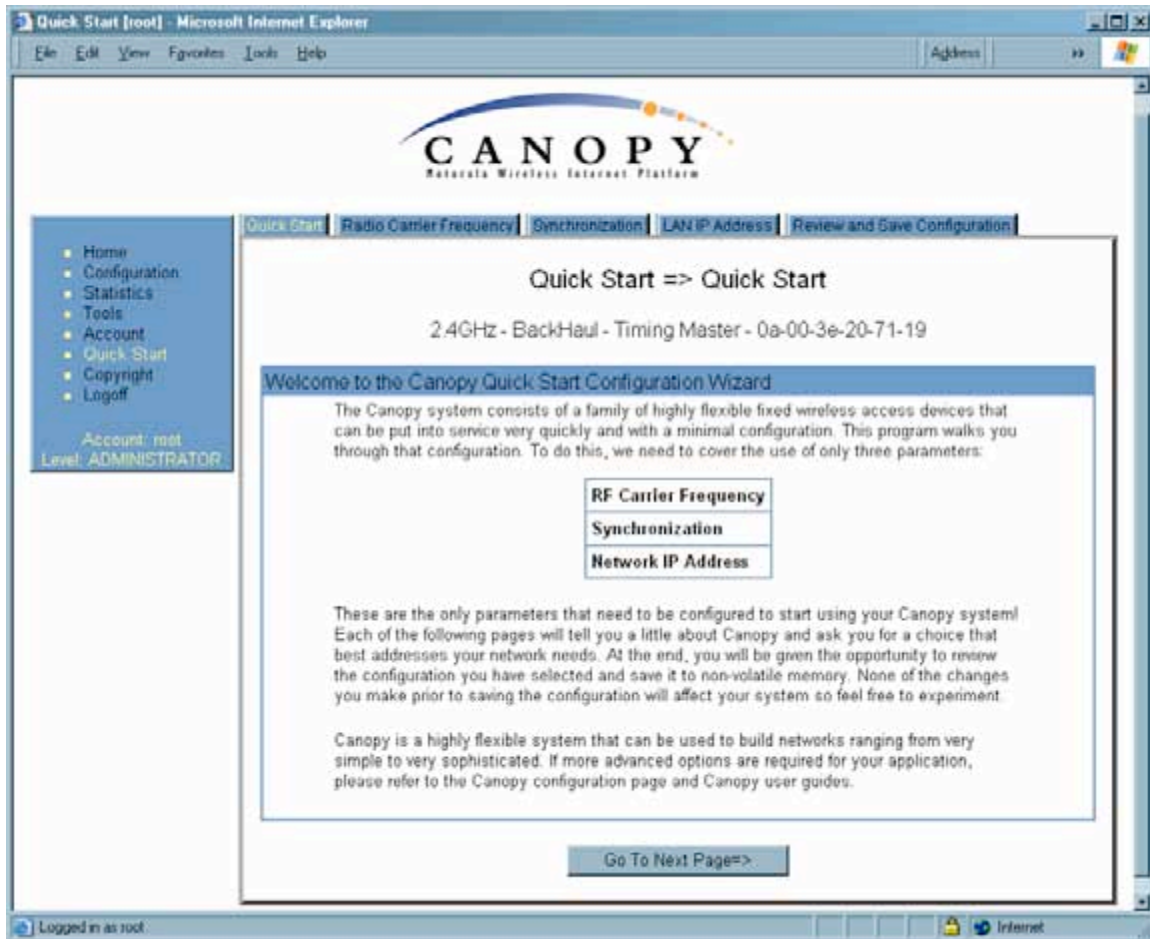


Figure 62: Quick Start tab of BHM, example

Quick Start is a wizard that helps you to perform a basic configuration that places a BHM into service. Only the following variables must be configured:

- **RF Carrier Frequency**
- **Synchronization**
- **Network IP Address**

In each page under Quick Start, you can

- specify the settings to satisfy the requirements of the network.
- review the configuration selected.
- save the configuration to non-volatile memory.

Proceed with the test setup as follows.

**Procedure 13: Using Quick Start to configure the BHs for test**

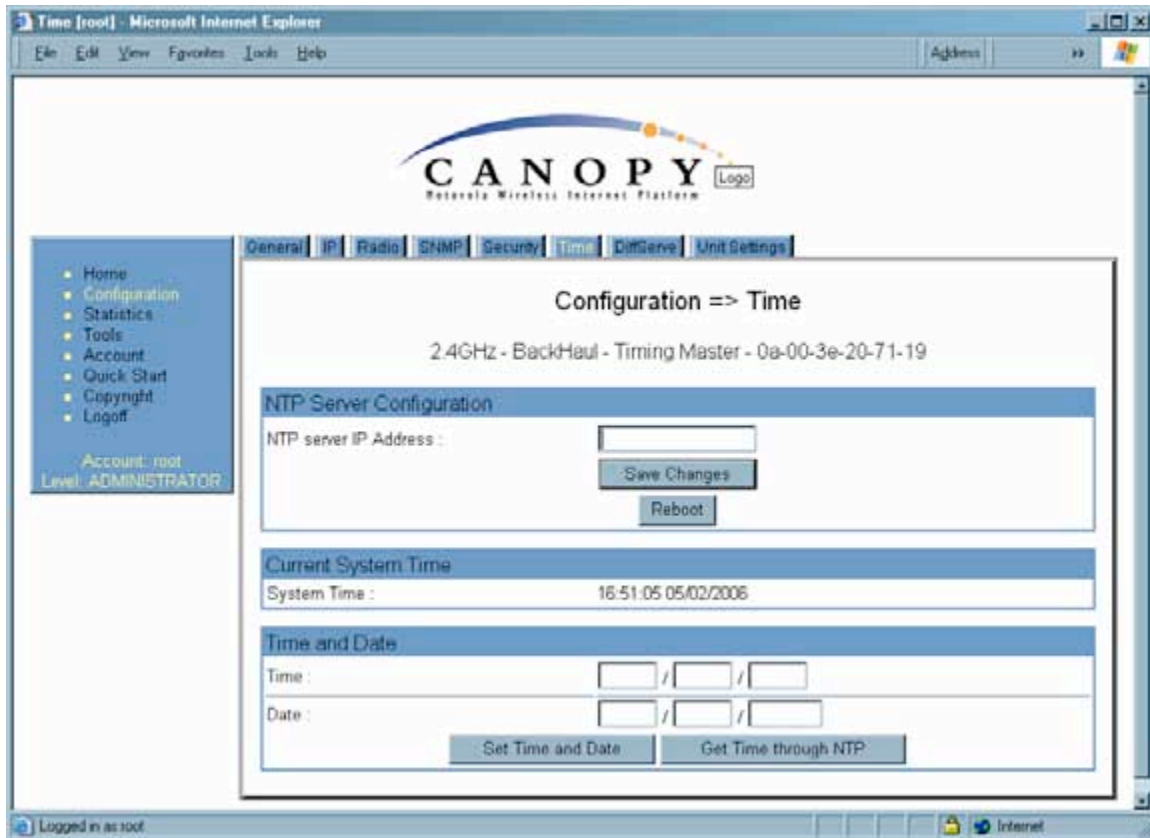
1. At the bottom of the Quick Start tab, click the **Go To Next Page =>** button.  
*RESULT:* The BHM responds by opening the RF Carrier Frequency tab.
2. From the pull-down menu in the lower left corner of this page, select a frequency for the test.
3. Click the **Go To Next Page =>** button.  
*RESULT:* The BHM responds by opening the Synchronization tab.
4. At the bottom of this page, select **Generate Sync Signal**.
5. Click the **Go To Next Page =>** button.  
*RESULT:* The BHM responds by opening the LAN IP Address tab.
6. At the bottom of this tab, either
  - specify an **IP Address**, **Subnet Mask**, and **Gateway IP Address** for management of the BHM and leave the **DHCP State** set to **Disabled**.
  - set the **DHCP State** to **Enabled** to have the IP address, subnet mask, and gateway IP address automatically configured by a domain name server (DNS).
7. Click the **Go To Next Page =>** button.  
*RESULT:* The BHM responds by opening the Review and Save Configuration tab.
8. Ensure that the initial parameters for the BHM are set as you intended.
9. Click the **Save Changes** button.
10. On the left side of the tab, click the **Configuration** button.  
*RESULT:* The BH responds by opening the General tab of its Configuration page.
11. In the **Timing Mode** parameter, select **Timing Master**.
12. Click the **Save Changes** button.
13. Click the **Reboot** button.  
*RESULT:* The BHM responds with the message **Reboot Has Been Initiated....** This BH is now forced to provide sync for the link and has a distinct set of web interface pages, tabs, and parameters for the role of BHM.
14. Wait until the indicator LEDs are not red.
15. Trigger your browser to refresh the page until the BHM redisplay the General Status tab of its Home page.
16. Repeat these steps to configure the other BH in the pair to be a BHS, selecting **Timing Slave** in Step 11.

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

Canopy encourages you to experiment with the interface. Unless you save a configuration and reboot the BHM after you save the configuration, none of the changes are effected.

#### 16.4.2 Time Tab of the BHM

To proceed with the test setup, in the BHM, click the **Configuration** button on the left side of the General Status tab. The BHM responds by opening its Configuration page to the General tab. Click the Time tab. An example of this tab is displayed in [Figure 63](#).



**Figure 63: Time tab of BHM, example**

To have each log in the BHM correlated to a meaningful time and date, either a reliable network element must pass time and date to the BHM or you must set the time and date whenever a power cycle of the BHM has occurred. A network element passes time and date in any of the following scenarios:

- A connected CMM2 passes time and date (GPS time and date, if received).
- A connected CMMmicro passes the time and date (GPS time and date, if received), but only if the CMMmicro is operating on CMMmicro Release 2.1 or later release. (These releases include an NTP server functionality.)
- A separate NTP server is addressable from the BHM.

If the BHM should derive time and date from either a CMMmicro or a separate NTP server, enter the IP address of the CMMmicro or NTP server on this tab. To force the BHM to derive time and date before the first (or next) 15-minute interval query of the NTP server, click **Get Time through NTP**.

If you enter a time and date, the format for entry is

Time : 

<i>hh</i>
-----------

 / 

<i>mm</i>
-----------

 / 

<i>ss</i>
-----------

Date : 

<i>MM</i>
-----------

 / 

<i>dd</i>
-----------

 / 

<i>YYYY</i>
-------------


where

- hh* represents the two-digit hour in the range 00 to 24
- mm* represents the two-digit minute
- ss* represents the two-digit second
- MM* represents the two-digit month
- dd* represents the two-digit day
- YYYY* represents the four-digit year

Proceed with the test setup as follows.

**Procedure 14: Setting up the BHS for test**

1. Enter the appropriate information in the format shown above.
2. Click the **Set Time and Date** button.  
*NOTE:* The time displayed at the top of this page is static unless your browser is set to automatically refresh.
3. In one hand, securely hold the top (larger shell) of the BH that you intend to deploy as a timing slave. With the other hand, depress the lever in the back of the base cover (smaller shell). Remove the base cover.
4. Plug one end of a CAT 5 Ethernet cable into the BHS.
5. Plug the other end of the Ethernet cable into the jack in the pig tail that hangs from the power supply.
6. Roughly aim the BHS toward the BHM.



**WARNING!**  
From this point until you remove power from the BHS, stay at least as far from the BHS as the minimum separation distance specified in [Table 37](#) on Page [169](#).

7. Plug the power supply into an electrical outlet.
8. Back at the computing device, on the left side of the BHM Time tab, click the **Home** button. When the Home page opens to the General Status tab, click the **Remote Subscribers** tab.  
*RESULT:* The BHM opens the Remote Subscribers tab. An example of this tab is shown in [Figure 64](#).

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



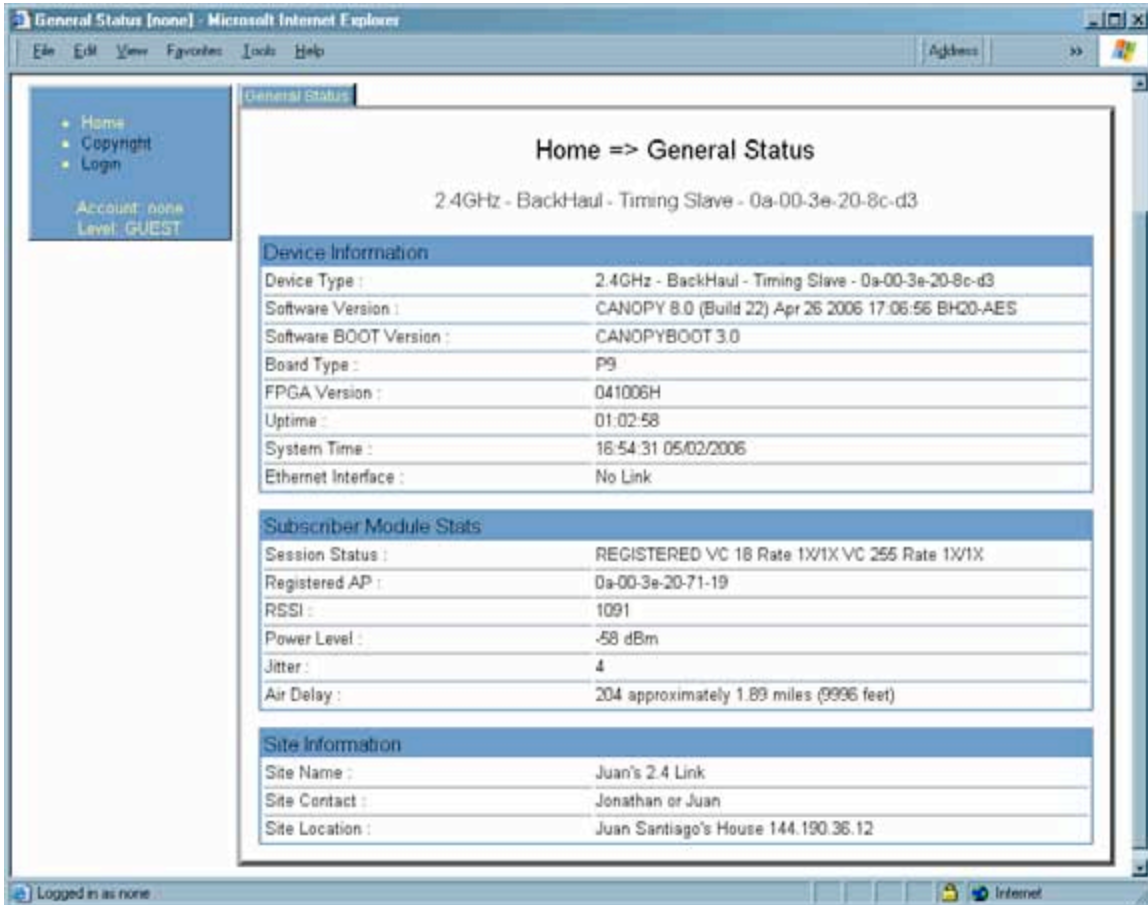


Figure 64: Remote Subscribers tab of BHM, example

### 16.4.3 Beginning the Test of Point-to-Point Links

To begin the test of your BH link, in the Remote Subscribers tab of the BHM, click the link to the BHS. The BHS GUI opens to the General Status tab of its Home page.

An example of the BHS General Status tab is displayed in [Figure 65](#).



**Figure 65: General Status tab of BHS, example**

The General Status tab provides information on the operation of this BHS. This is the tab that opens by default when you access the GUI of the BHS. The General Status tab provides the following read-only fields.

#### Device Type

This field indicates the type of the Canopy module. Values include the frequency band of the BHS, its module type, and its MAC address.

#### Software Version

This field indicates the Canopy system release, the time and date of the release, the modulation rate, and whether communications involving the module are secured by DES or AES encryption (see [Encrypting Canopy Radio Transmissions](#) on Page 369). If you request technical support, provide the information from this field.

**Software BOOT Version**

This field indicates the version of the CANOPYBOOT file. If you request technical support, provide the information from this field.

**Board Type**

This field indicates the series of hardware. See [Designations for Hardware in Radios](#) on Page 365.

**FPGA Version**

This field indicates the version of the field-programmable gate array (FPGA) on the module. When you request technical support, provide the information from this field.

**Uptime**

This field indicates how long the module has operated since power was applied.

**System Time**

This field provides the current time. When a BHS registers to a BHM, it inherits the system time, which is displayed in this field as GMT (Greenwich Mean Time).

**Ethernet Interface**

This field indicates the speed and duplex state of the Ethernet interface to the BHS.

**Session Status**

This field displays the following information about the current session:

- **Scanning** indicates that this SM currently cycles through the RF frequencies that are selected in the Radio tab of the Configuration page.
- **Syncing** indicates that this SM currently attempts to receive sync.
- **Registering** indicates that this SM has sent a registration request message to the AP and has not yet received a response.
- **Registered** indicates that this SM is both
  - registered to an AP.
  - ready to transmit and receive data packets.
- **Alignment** indicates that this SM is in an aiming mode. See [Table 41](#) on Page 179.

**Registered AP**

This field displays the MAC address of the BHM to which this BHS is registered.

**RSSI, Power Level, and Jitter**

The General Status tab shows the received **Power Level** in dBm and **Jitter**. Proper alignment maximizes **Power Level** and minimizes **Jitter**. As you refine alignment, you should favor lower jitter over higher dBm. For example, if coarse alignment gives the BHS 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, use the refined alignment, 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.

For historical relevance, the General Status tab also shows the **RSSI**, the unitless measure of power. Use **Power Level** and ignore **RSSI**. **RSSI** implies more accuracy and precision than is inherent in its measurement.



**NOTE:**

Unless the page is set to auto-refresh, the values displayed are from the instant the General Status tab was selected. To keep a current view of the values, refresh the browser screen or set to auto-refresh.

### **Air Delay**

This field displays the distance in feet between the BHS and the BHM. To derive the distance in meters, multiply the value of this parameter by 0.3048. Distances reported as less than 200 feet (61 meters) are unreliable.

### **Site Name**

This field indicates the name of the physical module. You can assign or change this name in the SNMP tab of the BHS Configuration page. This information is also set into the *sysName* SNMP MIB-II object and can be polled by an SNMP management server.

### **Site Contact**

This field indicates contact information for the physical module. You can provide or change this information in the SNMP tab of the BHS Configuration page. This information is also set into the *sysName* SNMP MIB-II object and can be polled by an SNMP management server.

### **Site Location**

This field indicates site information for the physical module. You can provide or change this information in the SNMP tab of the BHS Configuration page.

## **16.4.4 Continuing the Test of Point-to-Point Links**

To resume the test, perform the following steps.

### **Procedure 15: Verifying and recording information from the BHS**

1. Verify that the **Session Status** field of the General Status tab in the BHS indicates **REGISTERED**.  
*NOTE:* This indication confirms that the BHS is properly functional.
2. While your browser is set to the General Status tab, note (or print) the values of the following fields:
  - **Device type**
  - **Software Version**
  - **Software BOOT Version**
  - **Board Type**
  - **FPGA Version**

3. Systematically ensure that you can retrieve this data when you prepare to deploy the BHS.
4. Return your browser to the General Status tab of the BHM.

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

### 16.4.5 General Status Tab of the BHM

An example of a BHM General Status tab is displayed in [Figure 66](#).



Figure 66: General Status tab of BHM, example

The Status page provides information on the operation of the module. This is the default web page for the module. The Status page provides the following fields.

#### Device Type

This field indicates the type of the Canopy module. Values include the frequency band of the module, the module type, timing mode, and the MAC address of the module.

#### Software Version

This field indicates the software release that is operated on the module, the release date and time of the software release, the modulation rate capability, and whether the module

is secured by DES or AES encryption (see [Encrypting Canopy Radio Transmissions](#) on Page 369). When you request technical support, provide the information from this field.

#### Software BOOT Version

This field indicates the version of the CANOPYBOOT file. If you request technical support, provide the information from this field.

#### Board Type

This field indicates the series of hardware. See [Designations for Hardware in Radios](#) on Page 365.

#### FPGA Version

This field indicates the version of the field-programmable gate array (FPGA) on the module. When you request technical support, provide the information from this field.

#### Uptime

This field indicates how long the module has operated since power was applied.

#### System Time

This field provides the current time. If the BHM is connected to a CMM, then this field provides GMT (Greenwich Mean Time). The BHS that registers to the BHM inherits the system time.

#### Last NTP Time Update

If the Time & Date page of the module specifies that time should be received from an NTP server, then this field indicates when the time was last updated by a Network Time Protocol (NTP) server.

#### Ethernet Interface

This field indicates the speed and duplex state of the Ethernet interface to the module.

#### Registered SM Count

This field confirms that only one BHS is registered to the BHM.

#### GPS Sync Pulse Status

This field indicates the status of synchronization as follows:

- **Generating sync** indicates that the module is set to *generate* the sync pulse.
- **Receiving Sync** indicates that the module is set to *receive* a sync pulse from an outside source and is receiving the pulse.
- **ERROR: No Sync Pulse** indicates that the module is set to *receive* a sync pulse from an outside source and is not receiving the pulse.



**NOTE:**

When this message is displayed, the BHM transmitter is turned off to avoid self-interference within the Canopy system.

**Site Name**

This field indicates the name of the physical module. You can assign or change this name in the SNMP tab of the BHM Configuration page. This information is also set into the *sysName* SNMP MIB-II object and can be polled by an SNMP management server.

**Site Contact**

This field indicates contact information for the physical module. You can provide or change this information in the SNMP tab of the BHM Configuration page. This information is also set into the *sysName* SNMP MIB-II object and can be polled by an SNMP management server.

**Site Location**

This field indicates site information for the physical module. You can provide or change this information in the SNMP tab of the BHM Configuration page.

**Scheduling Type**

This field indicates the type of frame scheduler that is active in the BHM.

**16.4.6 Concluding the Test of Point-to-Point Links**

To conclude the test, perform the following steps.

**Procedure 16: Verifying and recording information from the BHM**

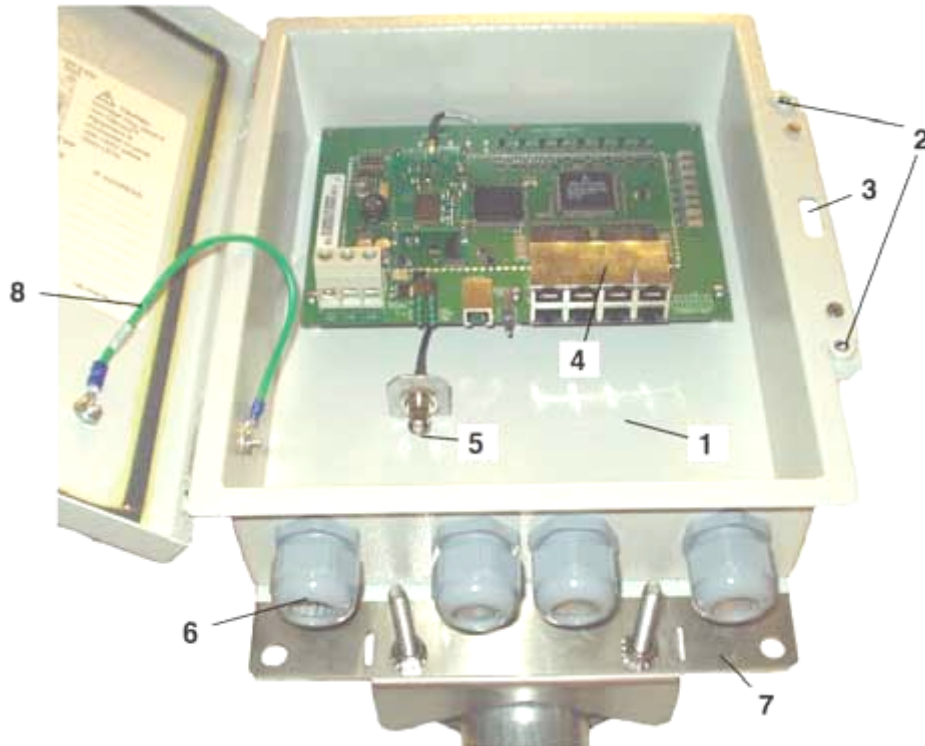
1. Confirm that the **GPS Sync Pulse Status** field indicates **Generating Sync**.  
*NOTE:* This indication confirms that the BHM is properly functional.
2. While your browser is set to this BHM Status page, note (or print) the values of the following fields:
  - **Device type**
  - **Software Version**
  - **Software BOOT Version**
  - **Board Type**
  - **FPGA Version**
3. Systematically ensure that you can retrieve this data when you prepare to deploy the BHM.

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

## 16.5 CONFIGURING A CMMMICRO FOR TEST

### 16.5.1 Setting up a CMMmicro

The layout of the CMMmicro is as shown in [Figure 67](#).




- 1 Weatherized enclosure
- 2 Thumb-screw/slot-screwdriver door fasteners
- 3 Punch-out for padlock
- 4 Ethernet switch and power module
- 5 Female BNC connector
- 6 Water-tight bulkhead connectors
- 7 Flange for attachment (stainless steel so it grounds to tower or building) using U bolts (provided) or other hardware such as screws or lag bolts or attachment straps (not provided).
- 8 Ground strap to ground door to enclosure

**Figure 67: CMMmicro layout**




Perform the following procedure to set up the CMMmicro.



**IMPORTANT!**  
Start with the 24-V DC power converter *unconnected* to AC.

**Procedure 17: Setting up a CMMmicro**

1. Connect the converter lead whose insulation has a white stripe to +V on the CMMmicro terminal block.
2. Connect the converter lead whose insulation is solid black to -V on the CMMmicro terminal block.
3. Connect the power converter to an AC receptacle using the AC power cord.
4. Wait until the green LED labeled RDY flashes.  
*NOTE:* This should occur in less than one minute and will indicate that the CMMmicro has transitioned from booting to normal operation.
5. Observe which, if any, Ethernet ports are powered, as indicated by a lit red LED to the right of the Ethernet port.  
*NOTE:* The position of this +24-V OUT LED is shown in [Figure 68](#) on Page 218.



**CAUTION!**  
Never connect any devices other than Canopy APs and BHs to a powered port. Powered ports are indicated by a red LED to the right of the port. (See Item 7 in [Figure 69](#) on Page 219.) A powered port has 24-V DC on Pins 7 and 8 and 24-V return on Pins 4 and 5. This can damage other networking equipment, such as a computer or a router.

6. On the 8-port Ethernet block of the CMMmicro, use either a straight-through or crossover Ethernet cable to connect any *unpowered* port (*without* the red LED lit) to a browser-equipped computer.  
*NOTE:* The CMMmicro auto-senses the cable type.
7. Verify these CMMmicro connections against [Figure 70](#) on Page 220.
8. Configure the computer to use DHCP, with no proxy in your network settings.
9. Open the browser.
10. In the address bar, enter 169.254.1.1 (the default IP address of the CMMmicro).  
*RESULT:* The browser displays the CMMmicro Status page.

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

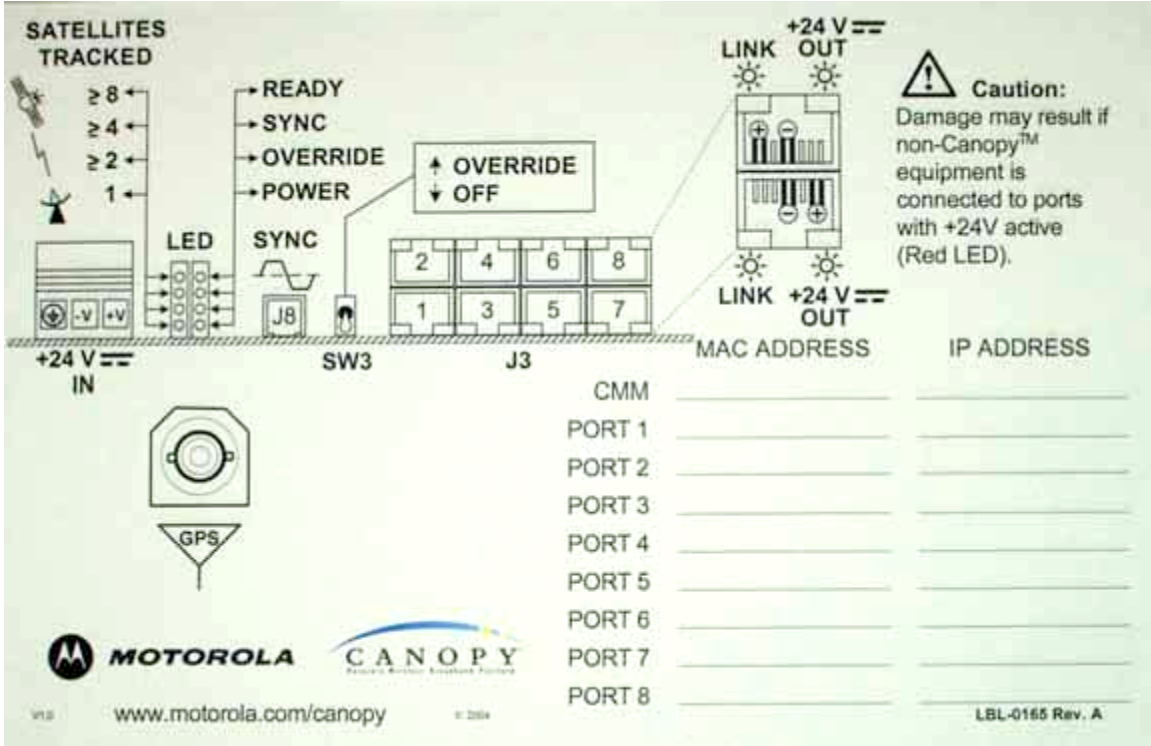
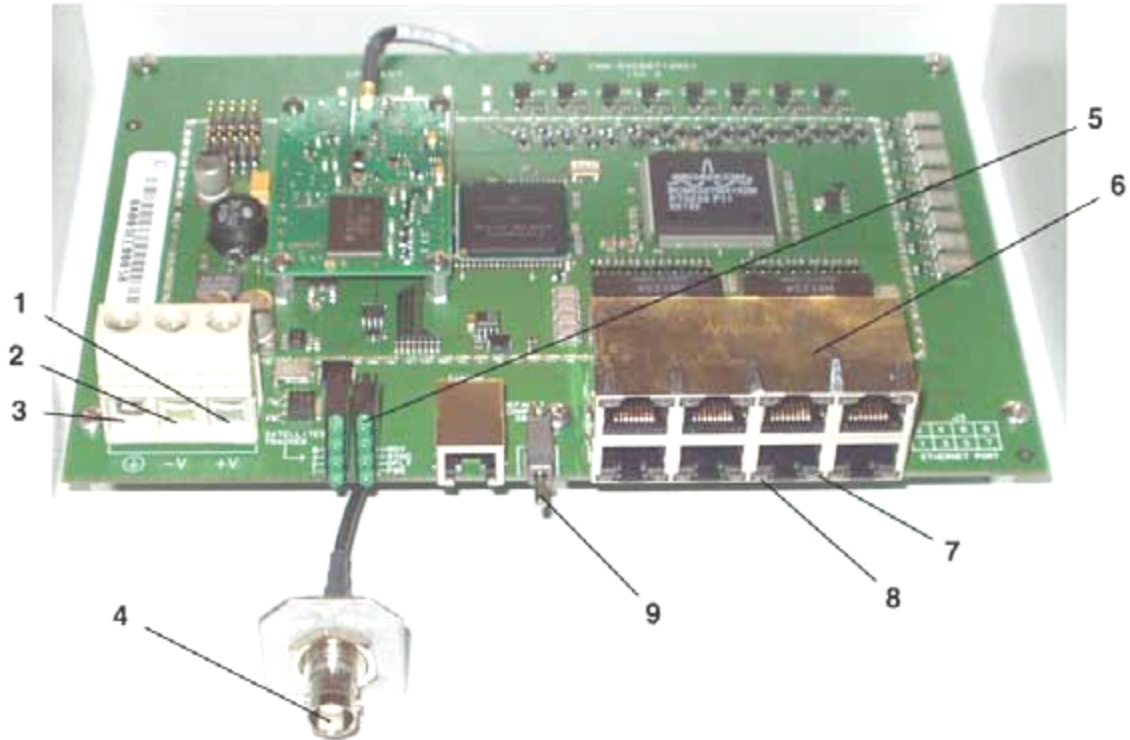


Figure 68: CMMmicro door label



- 1 24 V DC power connection on terminal block (+V).
- 2 24 V DC ground connection on terminal block (-V).
- 3 Ground bonding point for CMMmicro. Ground connection on terminal block, for grounding to Protective Earth (PE) ↓.
- 4 Female BNC connector for connecting to coax cable from GPS antenna.
- 5 Status display of eight green LEDs. The left LEDs show the number of satellites visible to the CMMmicro (1, 2,  $\geq 4$ , and  $\geq 8$ ), and the right LEDs show status:
  - RDY (Ready) – Flashing LED indicates CMMmicro software has booted and is operational. LED continues to flash during normal operation.
  - SYNC – Constant LED indicates CMMmicro is receiving signal from the GPS antenna and is able to derive sync.
  - DFLT (default) – Constant LED indicates CMMmicro has booted with Override Switch in down/override position, and therefore with default IP address (169.254.1.1) and no password.
  - PWR (power) – Constant LED indicates CMMmicro has power.
- 6 8-port Ethernet connection block with 2 LEDs per port indicating port status.
- 7 Constant red LED to the right of each port indicates the port is powered with 24 V DC (controlled by the CMMmicro Configuration page).
- 8 Constant green LED to the left of each port indicates the port is detecting Ethernet connectivity.
- 9 Override toggle switch, for overriding a lost or unknown IP address or password. Down is normal position, while rebooting in the up position brings the CMMmicro up with the default IP address (169.254.1.1) and no password required.

**Figure 69: CMMmicro circuit board**

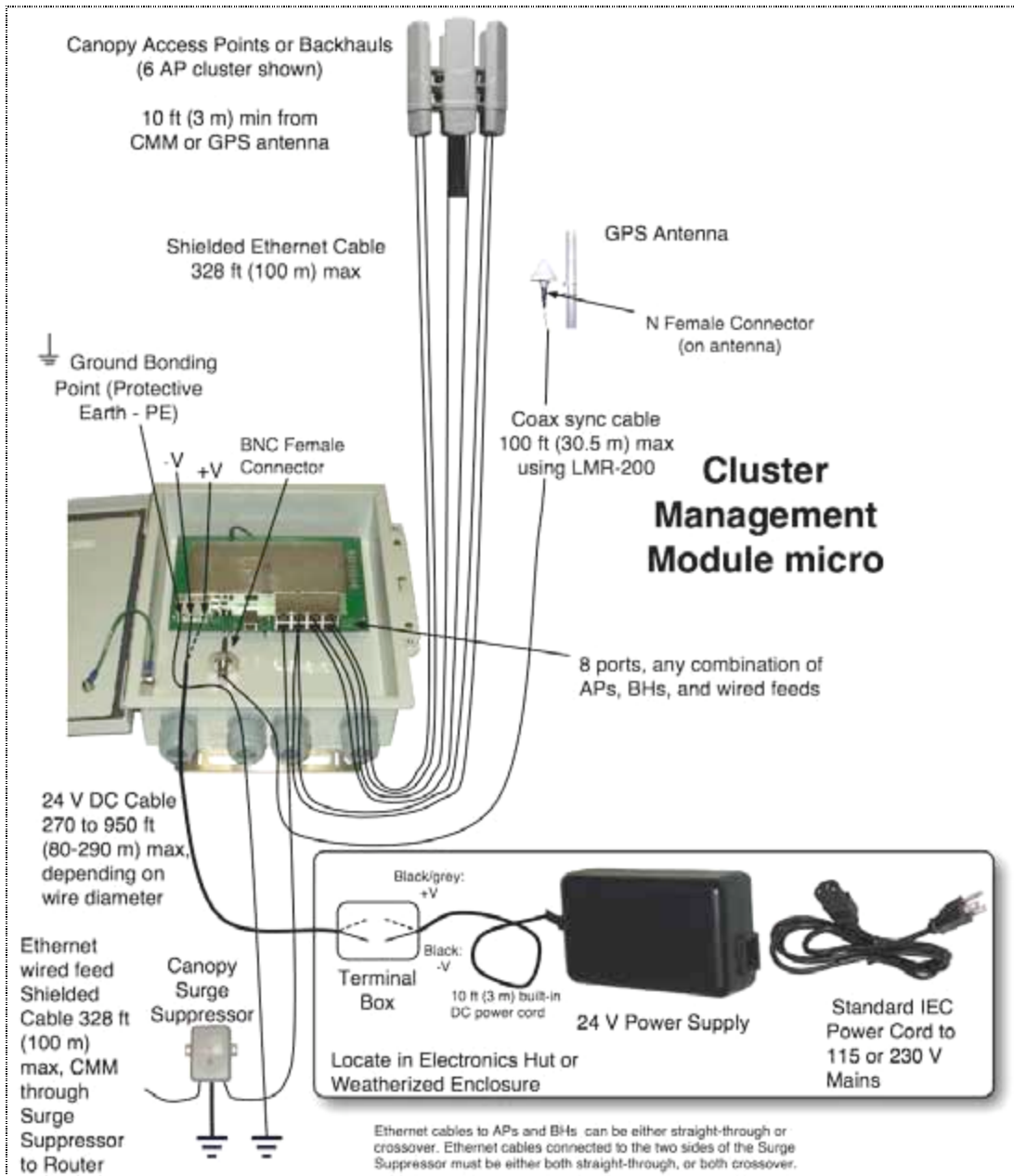


Figure 70: CMMmicro connections

### 16.5.2 Status Page of the CMMmicro

An example of a CMMmicro Status page is displayed in Figure 71.

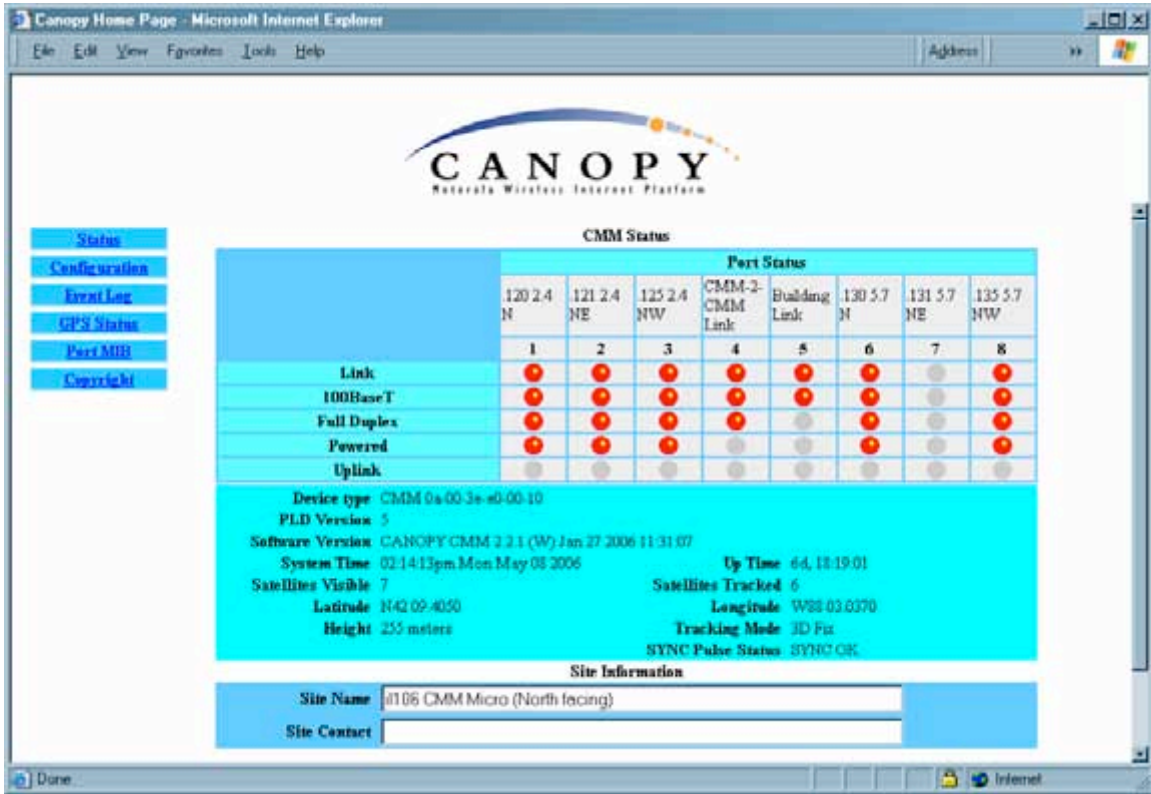


Figure 71: Status page of CMMmicro, example

The Status page provides information on the operation of this CMMmicro. This is the default web page for the CMMmicro. The Status page provides the following fields.

#### Link

A red dot indicates that the port is active and detects Ethernet traffic. A grey dot indicates that the port is not active and no traffic is detected.

#### 100BaseT

A red dot indicates that the port has auto-negotiated to a 100Base-T connection. A grey dot indicates that the port has auto-negotiated to a 10Base-T connection. (This convention is also used on many routers and network interface cards.) If the far end (an AP, a BH, a router) has been set to auto-negotiate, then the CMMmicro links at 100Base-T.

#### Full Duplex

A red dot indicates that the port has auto-negotiated to a Full Duplex connection. A grey dot indicates that the port has auto-negotiated to a Half Duplex connection. (This convention is also used on many routers and network interface cards.)

**Powered**

A red dot indicates that the port is powered with 24 V DC to provide power to an AP or BH. A grey dot indicates that the port is not powered. Port power is turned on and off in the **Port Power Control** parameter of the Configuration page. A CMMmicro comes from the factory with no Ethernet ports powered.

**CAUTION!**

Never connect any devices other than Canopy APs and BHs to a powered port. Powered ports are indicated by a red LED to the right of the port. (See Item 7 in [Figure 69](#) on Page 219.) A powered port has 24-V DC on Pins 7 and 8 and 24-V return on Pins 4 and 5. This can damage other networking equipment, such as a computer or a router.

**Uplink**

A red dot indicates this link has been configured as an uplink using the CMMmicro's Configuration page.

**Device Type**

This field displays the MAC address of the CMMmicro.

**PLD Version**

This field displays the version of the PLD (Programmable Logic Device) that is installed in the module. Before you request technical support, note this information.

**Software Version**

This field displays the version of the software that is installed in the module. Before you request technical support, note this information.

**System Time**

This field displays the current time. If the CMMmicro receives the signal from a GPS antenna, then this field expresses the time in Greenwich Mean Time (GMT).

**Satellites Visible**

This field displays how many satellites the GPS antenna sees.

**NOTE:**

This differs from the **Satellites Tracked** field (described below).

**Latitude**

If the CMMmicro receives the signal from a GPS antenna, then this field displays the latitude of the site.

**Height**

If the CMMmicro receives the signal from a GPS antenna, then this field displays the elevation (above sea level) of the GPS antenna.

**Uptime**

This field displays how much time has elapsed since the last boot of the CMMmicro.

**Satellites Tracked**

This field displays how many satellites the CMMmicro is tracking.

**Longitude**

If the CMMmicro receives the signal from a GPS antenna, then this field displays the longitude of the site.

**Tracking Mode**

If the CMMmicro receives the signal from a GPS antenna, then this field describes how the CMMmicro is tracking satellites.

**Sync Pulse Status**

This field indicates the status of sync pulse that the CMMmicro is currently able to provide to connected modules.

**Site Name**

This field displays administrative information that has been entered on the Configuration page of the CMMmicro.

**Site Contact**

This field displays administrative information that has been entered on the Configuration page of the CMMmicro.

### 16.5.3 Configuration Page of the CMMmicro


An example of the CMMmicro Configuration page is displayed in Figure 72.

Figure 72: Configuration page of CMMmicro, example

The Configuration web page contains all of the configurable parameters that define how the CMMmicro operates. The first line of information on the Configuration screen echoes



the **Device Type** from the Status web page.



**IMPORTANT!**  
Changes that are made to the following parameters become effective when you click the **Save Changes** button:

- **Port Configuration**
- **Description**
- **Power Port Control**
- **Webpage Auto Update**

When these parameters listed above have become effective, if you click the **Undo Saved Changes** button, the previous values are *not* restored.

Changes that are made to all other parameters become effective only after all of the following have occurred:

- you have clicked the **Save Changes** button.
- you click the **Reboot** button.
- the CMMmicro reboots.

**Procedure 18: Setting CMMmicro parameters for test**


To continue the test setup, configure

1. the **GPS Timing Pulse** parameter.
2. the **Lan1 IP** parameter.
3. the **Lan1 Subnet Mask** parameter.
4. the **Default Gateway** parameter.
5. the **Port Power Control** parameter.

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

**GPS Timing Pulse**

Select **Master**. (**Slave** is for future use.)



**IMPORTANT!**  
If the GPS Timing Pulse is set to **Slave**, the CMMmicro GPS receiver is disabled.

**Lan1 IP**

Enter the IP address to be associated with the Ethernet connection on this CMMmicro. The default address is 169.254.1.1. If you set and then forget this parameter, then you must both

1. physically access the module.

2. use the CMMmicro override toggle switch to electronically access the module configuration parameters at 169.254.1.1. See [Overriding Forgotten IP Addresses or Passwords on CMMmicro](#) on Page 375.

**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.

**LAN Subnet Mask**

Enter the appropriate subnet mask for the module to communicate on the network. The default value for this parameter is 255.255.255.0.

**Default Gateway**

Enter the appropriate gateway for the module to communicate on the network. The default for this parameter is 169.254.0.0.

**Port Configuration**

If you wish to force a port to a speed or duplex state, or to return the module to auto-negotiating speed and duplex state, change the selection for the port. The range of selections are defined in [Table 42](#).

**Table 42: Port Configuration selections for CMMmicro**

Selection	Result
Auto	The port attempts to auto-negotiate speed and duplex state. (This is the default and recommended setting.)
100FDX	The port is forced to 100 Mbps and full duplex.
100HDX	The port is forced to 100 Mbps and half duplex.
10FDX	The port is forced to 10 Mbps and full duplex.
10HDX	The port is forced to 10 Mbps and half duplex.

If you change this value for a port and then click **Save Changes**, then the change becomes effective immediately and the previous value is lost.

**Description**

You can enter text in this parameter (for example, text that helps you to associate the port number with the connected device.) If you change this value for a port and then click **Save Changes**, then the change becomes effective immediately and the previous value is lost.

**Power Port Control**

Ensure that power is off for every port that connects to a router, computer, or other network equipment. Turn on 24-V DC power for ports that connect to Canopy APs or BHs.

**CAUTION!**

Never connect any devices other than Canopy APs and BHs to a powered port. Powered ports are indicated by a red LED to the right of the port. (See Item 7 in [Figure 69](#) on Page 219.) A powered port has 24-V DC on Pins 7 and 8 and 24-V return on Pins 4 and 5. This can damage other networking equipment, such as a computer or a router.

If you change this value for a port and then click **Save Changes**, then the change becomes effective immediately and the previous value is lost.

**Display-Only Access**

To set this password, enter the same expression in both **Display-Only Access** fields for verification. When the web-based interface prompts for this password, no user name is required. However, when a telnet or FTP session prompts for this password, you must enter the user name `root` in addition to the password.

If you set and then forget the **Display-Only Access** password, then you must both

1. physically access the module.
2. use the CMMmicro override toggle switch to electronically access the module configuration parameters at 169.254.1.1. See [Overriding Forgotten IP Addresses or Passwords on CMMmicro](#) on Page 375.

**Full Access**

If you set the **Full Access** password, this password will allow

- telnet and FTP access to the module.
- *viewing or changing* the parameters of the module.

To set this password, enter the same expression in both **Full Access** fields for verification. When the web-based interface prompts for this password, no user name is required. However, when a telnet or FTP session prompts for this password, you must enter the user name `root` in addition to the password.

If you set and then forget the **Full Access** password, then you must both

1. physically access the module.
2. use the CMMmicro override toggle switch to electronically access the module configuration parameters at 169.254.1.1. See [Overriding Forgotten IP Addresses or Passwords on CMMmicro](#) on Page 375.

**NOTE:**

You can unset either password (revert the access to no password required). To do so, type a space into the field and reboot the module. You must enter any password twice to allow the system to verify that the password is not mistyped. After any password is set and a reboot of the module has occurred, a **Password Set** indicator appears to the right of the field.

**RECOMMENDATION:**

Note the passwords that you enter. Ensure that you can readily associate these passwords both with the module and with the other data that you store about the module.

**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.

If you change this value and then click **Save Changes**, then the change becomes effective immediately and the previous value is lost.

**SNMP Community String**

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

The **SNMP Community String** value is clear text and is readable by a packet monitor. Additional security derives from the configuration of the **SNMP Accessing Subnet**, **Trap Address**, and **Permission** parameters.

**SNMP Accessing Subnet**

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

**RECOMMENDATION:**

For more information on CIDR, execute an Internet search on "Classless Interdomain Routing."

The default treatment is to allow all networks access.

**Trap Address**

Specify the IP address (xxx.xxx.xxx.xxx) of one to ten servers (Prizm or NMS) to which trap information should be sent. Trap information informs the monitoring systems 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.

**Permission**

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 CMMmicro Configuration page also provides the following buttons.

**Enable 802.1Q Tagging**

Once 802.1Q Tagging is enabled and an 802.1Q VLAN ID is set, only frames that are VLAN tagged with the configured tag value will be accepted by the management controller of the CMMmicro. All frames outgoing from the management controller of the CMMmicro will have an 802.1Q VLAN tag, set to the configured VLAN ID.

**802.1Q VLAN ID**

Once 802.1Q Tagging is enabled and an 802.1Q VLAN ID is set, only frames that are VLAN tagged with the configured tag value will be accepted by the management controller of the CMMmicro. All frames outgoing from the management controller of the CMMmicro will have an 802.1Q VLAN tag, set to the configured VLAN ID.

**VLAN Port Configuration**

Each column in the VLAN Port Configuration section of [Figure 72](#) corresponds to a port. Checkboxes in each column control which ports can transmit traffic that arrives on the (column) port. For example, in the first column if only Port 2 is checked, then Port 1 (column 1) will only be allowed to send data out on Port 2 (checked box). Port 2 (second column) is able to send data out on all other ports. All other ports, meanwhile, are only allowed to send data out on Port 2. This configuration is also known as an Uplink configuration for Port 2.

Each direction (for example, port 1 to port 2 versus port 2 to port 1) must be configured separately. It is possible to configure a port to send data to a second port, but not allow

the second port to send data back to the first port (for example, check Port 8 in the Port 2 column, but do not check Port 2 in the Port 8 column). These settings should be changed with caution, and with two-way communication in mind.

In all cases, even when not checked, all ports will still be able to communicate with the CMMmicro management controller.

Setting (checking) any Uplink Port checkboxes (see [Figure 72](#)) will override VLAN Port Configuration settings. If you desire complete control on a port-by-port basis using VLAN Port Configuration, all Uplink Port boxes must be unchecked in the Uplink Port section.

**Save Changes, Undo Saved Changes, Set to Defaults, Reboot**

The effects of clicking these buttons are defined in [Table 43](#).

**Table 43: When changes become effective in CMMmicro**

For these parameters...	clicking this button...	has this effect.
<b>Port Configuration</b> <b>Description</b> <b>Power Port Control</b> <b>Webpage Auto Update</b>	<b>Save Changes</b>	Any change becomes effective immediately and any previous setting is lost.
	<b>Undo Saved Changes</b>	No change is undone, and no previous setting is restored.
	<b>Set to Defaults</b>	The default setting is not restored.
	<b>Reboot</b>	No change that is not already effective becomes effective.
Any other parameter	<b>Save Changes</b>	Any change is recorded into flash memory but does not become effective immediately, and any previous setting can be restored.
	<b>Undo Saved Changes</b>	Any change recorded into flash memory is undone, and the previous setting is restored.
	<b>Set to Defaults</b>	The default setting is restored.
	<b>Reboot</b>	Any change recorded in flash memory (and not later undone) becomes effective.

In addition, when you click **Reboot**, the following events occur and are logged:

- The CMMmicro reboots.
- Any AP or BH that receives power from the CMMmicro loses power and thus also reboots.
- Any AP or BH that does not receive power but receives sync from the CMMmicro loses and then regains sync.

### 16.5.4 Configuring Modules for Connection to CMMmicro

After configuring the CMMmicro, configure the APs and BHs as follows. In each AP or BH that connects to a CMMmicro, you must set the **Sync Input** parameter of the Configuration page of that module to **Sync to Received Signal (Power Port)**. See

- [Sync Input](#) on Page 237.
- [Sync Input](#) on Page 296.

### 16.5.5 Event Log Page of the CMMmicro

This page may contain information that can be useful under the guidance of Canopy technical support. For this reason, the operator *should not* clear the contents of this page before contacting technical support.

### 16.5.6 GPS Status Page of the CMMmicro

An example of the CMMmicro GPS Status page is displayed in [Figure 73](#).

The screenshot shows a web browser window titled "Canopy Home Page - Microsoft Internet Explorer". The main content area displays the Canopy logo and a navigation menu on the left with links for Status, Configuration, Event Log, GPS Status, Port MIB, and Copyright. The "GPS Status" page is active, showing the following data:

GPS Status			
SYNC Pulse Status	SYNC OK	Tracking Mode	3D Fix
GPS Time	14:44:36	GPS Date	05/08/2006
Satellites Tracked	7	of Satellites Visible	7
Height	264 meters	Antenna Connection	OK
Latitude	N42 09.4040	Invalid Msg	1
Longitude	W88 03.0370	Restart Count	0

Below the GPS Status section is the "GPS Receiver Information" section, which contains the following text:

```

COPYRIGHT 1991-2003 MOTOROLA INC.
SFTW P/N # 61-G10268A
SOFTWARE VER # 2
SOFTWARE REV # 1
SOFTWARE DATE APR 16 2003
MODEL # P283T12T12
HWDR P/N # 2
SERIAL # P06X8V
MANUFACTUR DATE 3L11

```

Figure 73: GPS Status page of CMMmicro, example

The GPS Status page provides information from the GPS antenna and information about the GPS receiver in the CMMmicro.

#### Antenna Connection

This field displays the status of the signal from the antenna as follows:

- **OK** indicates that the GPS interface board is detecting an incoming signal on the coaxial cable from the GPS antenna.

- **No Antenna** indicates the GPS interface board is not detecting any incoming signal.

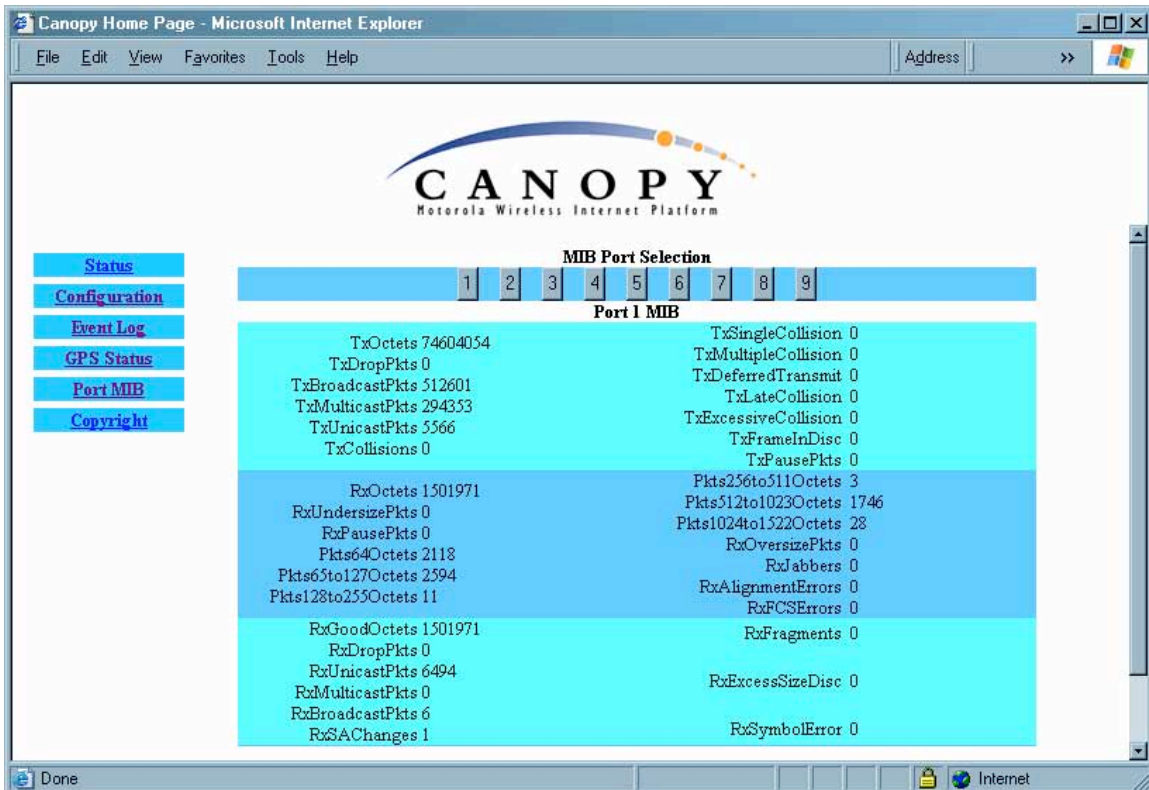
The other GPS Status fields are described under [Satellites Visible](#) on Page 222.

### GPS Receiver Information

This field displays information about the GPS interface board.

## 16.5.7 Port MIB Page of the CMMmicro

An example of the Port MIB (Ethernet statistics) web page is displayed in [Figure 74](#).



**Figure 74: Port MIB page of CMMmicro, example**

The Port MIB page displays Ethernet statistics and traffic information for the ports on the managed switch. To display the port statistics, click on a port number.

Ports 1 through 8 are the regular ports, connected to APs, BHs, or other network elements. Port 9 is the connection between the managed switch and the CMMmicro processor. Thus, updates to interface pages, SNMP activities, and FTP and telnet sessions create traffic on Port 9.

These Ethernet statistics can also be retrieved from the CMMmicro by a Network Management Station using SNMP. During advanced troubleshooting, this information can be useful as you see the activity on a single port or as you compare activity between ports of the CMMmicro.



## 17 PREPARING COMPONENTS FOR DEPLOYMENT

Your test of the modules not only verified that they are functional, but also yielded data that you have stored about them. Most efficiently preparing modules for deployment involves

- retrieving that data.
- systematically collecting the data into a single repository, while keeping a strong (quick) association between the data and the module.
- immediately merging module access data into this previously stored data.

### 17.1 CORRELATING COMPONENT-SPECIFIC INFORMATION

You can use the data that you noted or printed from the Status pages of the modules to

- store modules for future deployment.
- know, at a glance, how well-stocked you are for upcoming network expansions.
- efficiently draw modules from stock for deployment.
- plan any software updates that you
  - wish to perform to acquire features.
  - need to perform to have the feature set be consistent among all modules in a network expansion.

You can make these tasks even easier by collecting this data into a sortable database.

### 17.2 ENSURING CONTINUING ACCESS TO THE MODULES

As you proceed through the steps under [Configuring for the Destination](#) on Page 235, you will set values for parameters that specify the sync source, data handling characteristics, security measures, management authorities, and other variables for the modules. While setting these, you will also tighten access to the module, specifically in

- the **Color Code** parameter of Configuration page
- the **Display-Only Access** and **Full Access** password parameters of the Configuration page.
- the addressing parameters of the IP Configuration page.

Before you set these, consider whether and how you may want to set these by a self-devised scheme. A password scheme can help you when you have forgotten or misfiled a password. An IP addressing scheme may be essential to the operation of your network and to future expansions of your network.

As you set these, note the color code and note or print the parameters you set on the Configuration page tabs. Immediately associate them with the following previously stored data about the modules:

- device type, frequency band, and MAC address
- software version and encryption type
- software boot version
- FPGA version



## 18 CONFIGURING FOR THE DESTINATION

### 18.1 CONFIGURING AN AP FOR THE DESTINATION

If an ADMINISTRATOR-level password has been set in the AP, you must log into the module before you can configure its parameters. See [Managing Module Access by Passwords](#) on Page 371.

#### 18.1.1 General Tab of the AP

An example of an AP General tab is displayed in [Figure 75](#).

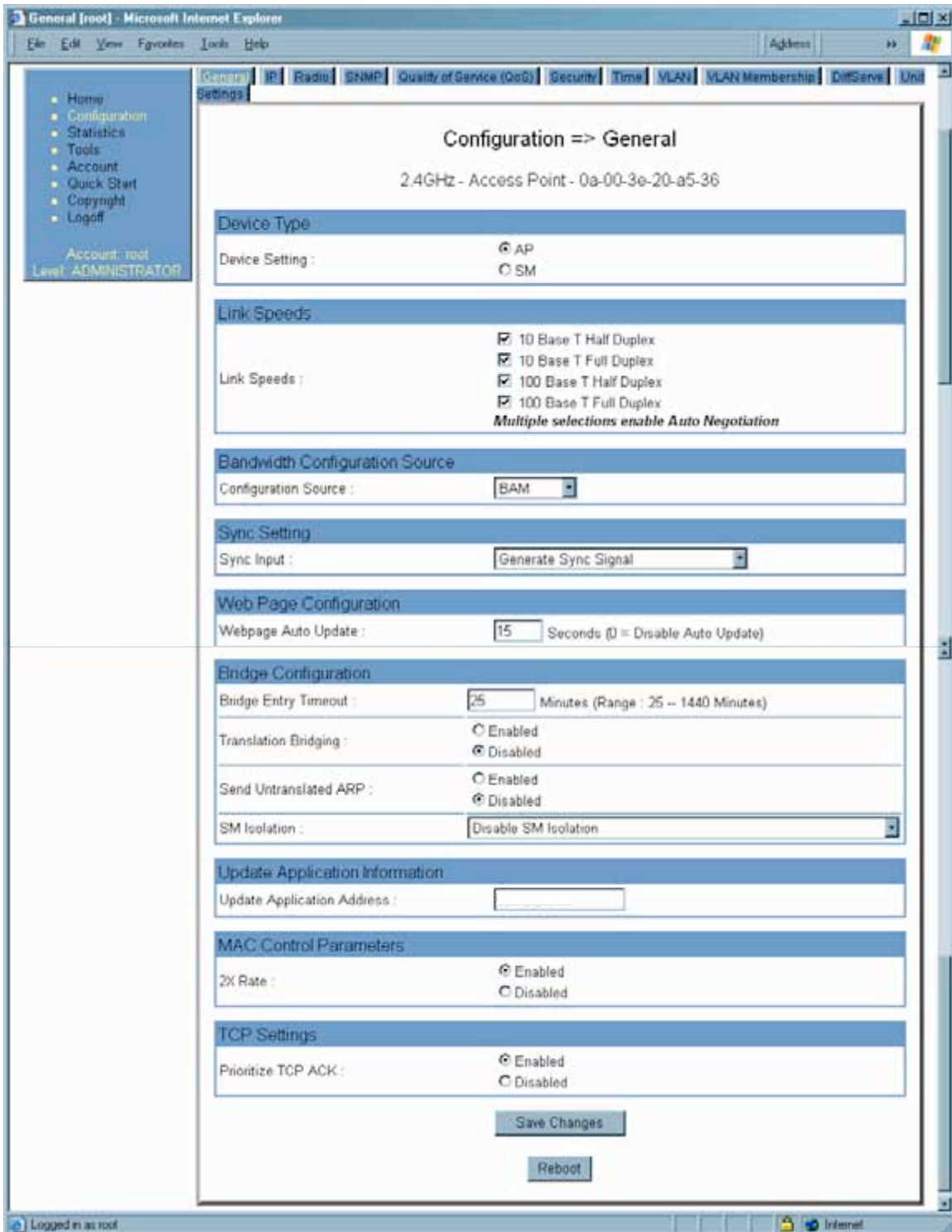


Figure 75: General tab of AP, example

The General tab of the AP contains many of the configurable parameters that define how the AP and the SMs in the sector operate. As shown in [Figure 75](#), you may set the Configuration page parameters as follows.

### Device Setting

You can temporarily transform an AP into an SM and thereby use the spectrum analyzer functionality. See [Using the AP as a Spectrum Analyzer](#) on Page 364. Otherwise, the selection for this parameter is **AP**.

### 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.

### Configuration Source

See [Setting the Configuration Source](#) on Page 292.



#### **CAUTION!**

Do not set this parameter to **BAM** where both

- a BAM release earlier than 2.1 is implemented.
- the **All Local SM Management** parameter (in the VLAN Configuration page of the AP) is set to **Enable**.

This combination causes the SMs to become unmanageable, until you gain direct access with an Override Plug and remove this combination from the AP configuration.

### Sync Input

Specify the type of synchronization for this AP to use:

- Select **Sync to Received Signal (Power Port)** to set this AP to receive sync from a connected CMMmicro.
- Select **Sync to Received Signal (Timing Port)** to set this AP to receive sync from a connected CMM2, an AP in the cluster, an SM, or a BH timing slave.
- Select **Generate Sync Signal** where the AP does not receive sync, and no other AP or BHM is active within the link range.

### 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. The Bridge Entry Timeout should be a longer period than the ARP (Address Resolution Protocol) cache timeout of the router that feeds the network.

**CAUTION!**

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

**Translation Bridging**

If you want the Translation Bridging feature, select **Enabled**. This has numerous implications. For a full description of them, see [Uplink Frame Contents](#) on Page 81.

**Send Untranslated ARP**

If the **Translation Bridging** parameter is set to **Enabled**, then the **Send Untranslated ARP** parameter can be

- disabled, so that the AP will overwrite the MAC address in Address Resolution Protocol (ARP) packets before forwarding them.
- enabled, so that the AP will forward ARP packets regardless of whether it has overwritten the MAC address.

See [Uplink Frame Contents](#) on Page 81 and [Address Resolution Protocol](#) on Page 162.

If the **Translation Bridging** parameter is set to **Disabled**, then the **Send Untranslated ARP** parameter has no effect.

**SM Isolation**

Prevent or allow SM-to-SM communication by selecting from the following drop-down menu items:

- **Disable SM Isolation** (the default selection). This allows full communication between SMs.
- **Block SM Packets from being forwarded**. This prevents both multicast/broadcast and unicast SM-to-SM communication.
- **Block and Forward SM Packets to Backbone**. This not only prevents multicast/broadcast and unicast SM-to-SM communication but also sends the packets, which otherwise would have been handled SM to SM, through the Ethernet port of the AP.

**Update Application Address**

Enter the address of the server to access for software updates on this AP and registered SMs.

**2X Rate**

See [2X Operation](#) on Page 89.

**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. See [AP-SM Links](#) on Page 99.

The General tab also provides the following buttons.

### Save Changes

When you click this button, any changes that you made on the 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.

## 18.1.2 IP Tab of the AP

An example of the IP tab of the AP is displayed in [Figure 76](#).

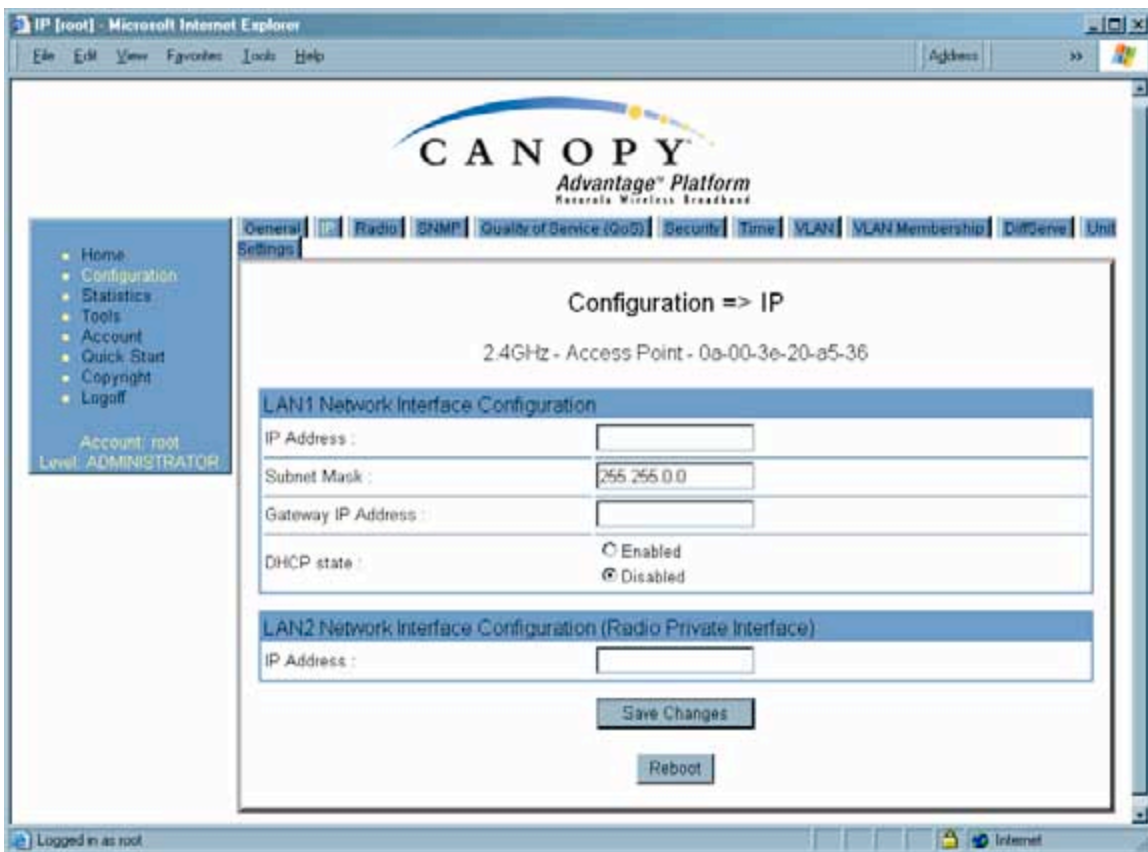


Figure 76: IP tab of AP, example

You may set the IP tab parameters as follows.

### LAN1 Network Interface Configuration, IP Address

Enter the *non-routable* IP address to associate with the Ethernet connection on this AP. (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 375.



#### **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 AP 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 AP to communicate with the network. The default gateway is 169.254.0.0.

The values of these four LAN1 network interface configuration parameters are displayed read only along with the Ethernet speed and duplex state on the Network Interface tab of the Home page in the AP.

### 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.

### LAN2 Network Interface Configuration (RF Private Interface), IP Address

You should not change this parameter from the default AP private IP address of 192.168.101.1. A /24 CIDR subnet is used to communicate with each of the SMs that are registered. The AP uses a combination of the private IP and the LUID (logical unit ID) of the SM.

For example, if an SM is the first to register in an AP, and another SM registers later, then the AP whose Private IP address is 192.168.101.1 uses the following SM Private IP addresses to communicate to each:

SM	LUID	Private IP
First SM registered	2	192.168.101.2
Second SM registered	3	192.168.101.3



**NOTE:**

Where space is limited for subnet allocation, be advised that an SM *need not* have an operator-assigned IP address. The SM is directly accessible without an LUID if either the SM **Color Code** parameter is set to 0 or the AP has a direct Ethernet connection to the SM.

The IP Configuration page 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.

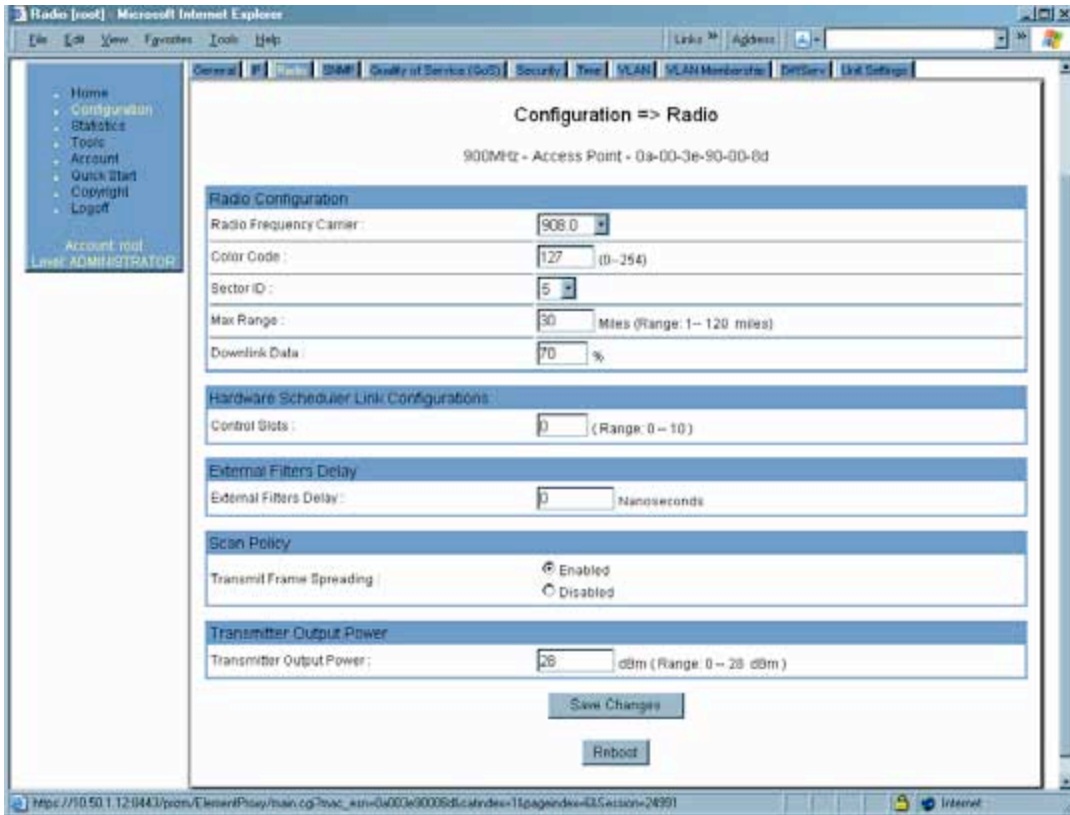
**Reboot**

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.

**18.1.3 Radio Tab of the AP**

An example of the Radio tab of the AP is shown in [Figure 77](#).



**Figure 77: Radio tab of AP (900 MHz), example**

The Radio tab of the AP contains some of the configurable parameters that define how the AP operates. As shown in [Figure 77](#), you may set the Radio tab parameters as follows.

### Radio Frequency Carrier

Specify the frequency for the module to transmit. The default for this parameter is **None**. (The selection labeled **Factory** requires a special software key file for implementation.) For a list of channels in the band, see the drop-down list or [Considering Frequency Band Alternatives](#) on Page 136.

### 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 an SM to register to only a specific AP, even where the SM can communicate with multiple APs. 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.

### Sector ID

Specify a number in the range 1 to 6 to associate with this AP. The Sector ID setting does not affect the operation of the AP. On the AP Evaluation tab of the Tools page in the SM, the **Sector ID** field identifies the AP that the SM sees. The following steps may be useful:

- Assign a unique Sector ID to each sector in an AP cluster.
- Repeat the assignment pattern throughout the entire Canopy system.

### Max Range

Enter a number of miles (or kilometers divided by 1.61, then rounded to an integer) for the furthest distance from which an 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. See [Table 24](#) on Page 100.

Regardless of this distance, the SM must meet the minimum requirements for an acceptable link. If the AP is in cluster, then you *must* set this parameter on all other APs in the cluster exactly the same, except as described in the NOTE admonition below. The default value of this parameter is 2 miles (3.2 km).

For APs in the non 900-MHz frequency band ranges, although the typical maximum range where an SM is deployed with a reflector is 15 miles (24 km), you can set this parameter to as far as 30 miles (48 km). Without increasing the power or sensitivity of the

AP or SM, the greater value allows you to attempt greater distance where the RF environment and Fresnel zone<sup>6</sup> are especially clear.

A value of 15 for this parameter decreases the number of available data slots by 1. With a higher value, the number is further decreased as the AP compensates for the expected additional air delay.



**NOTE:**

In a cluster where at least one AP has **Scheduling** set to **Software** and at least one to **Hardware**, you must use the Frame Calculator web page to coordinate the transmit and receive times and you may further need to adjust the value of the **Max Range** parameter for individual APs in the cluster to avoid self interference. See [Using the Frame Calculator Tool \(All\)](#) on Page 438.

### 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 6 Mb, then 75% specified for this parameter allocates 4.5 Mb for the downlink and 1.5 Mb for the uplink. The default for this parameter is 75%.



**CAUTION!**

You must set this parameter exactly the same for all APs in a cluster.

### Control Slots

The recommended number of control slots is as stated in [Table 44](#).

**Table 44: Control slot settings for all APs in cluster**

Number of SMs that Register to the AP	Number of Control Slots Recommended
1 to 10	0
11 to 50	1
51 to 150	2
151 to 200	3

Slots reserved for control are used for only SM service requests. For data, the hardware scheduler uses unreserved slots first, then any unused slots are available with any reserved slots to the SMs for service requests.

<sup>6</sup> See [Noting Possible Obstructions in the Fresnel Zone](#) on Page 132.

If too few reserved control slots are specified, then latency increases in high traffic periods. If too many are specified, then the maximum capacity is unnecessarily reduced.

### External Filters Delay

This parameter is present in only 900-MHz modules and can have effect in only those that have interference mitigation filter(s). Leave this value set to **0**, regardless of whether the AP has an interference mitigation filter.

### Transmit Frame Spreading

Where multiple AP clusters operate in the same frequency band range and same geographical area, select **Enable**. Then SMs between two APs can register in the assigned AP (do not register in another AP).

Where multiple AP clusters *do not* operate in the same frequency band range and same geographical area, select **Disable**, but observe the following caveat.



#### **IMPORTANT!**

SM throughput is 10% greater with this feature disabled. However, if you disable **Transmit Frame Spreading** where this feature was previously enabled, monitor the zone for interference over a period of days to ensure that this action has not made any SMs sensitive to the wrong beacon.

With this selection enabled, the AP does not transmit a beacon in each frame, but rather transmits a beacon in only pseudo-random frames in which the SM expects the beacon. This allows multiple APs to send beacons to multiple SMs 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 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.

### 18.1.4 SNMP Tab of the AP

An example of the SNMP tab of the AP is displayed in Figure 78.



Figure 78: SNMP tab of AP, example

You may set the SNMP tab parameters as follows.

### Community String

Specify a control string that allows an Network Management Station (NMS) to access SNMP information. 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 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.”

### Trap Address 1 to 10

Specify ten or fewer IP addresses (xxx.xxx.xxx.xxx) to which SNMP traps should be sent. Traps inform Prizm 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 you want sync status traps (sync lost and sync regained) sent to Prizm or an NMS, select **Enabled**. If you want these traps suppressed, select **Disabled**.

### Trap Enable, Session Status

If you want session status traps sent to Prizm or an NMS, select **Enabled**. For the names and descriptions of session status traps, see [Traps Provided in the Canopy Enterprise MIB on Page 404](#). If you want these traps suppressed, select **Disabled**.

### Read Permissions

Select **Read Only** if you wish to disallow any parameter changes through SNMP (for example, from 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 PrizmEMS 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 PrizmEMS 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 PrizmEMS 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 this tab are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

**Reboot**

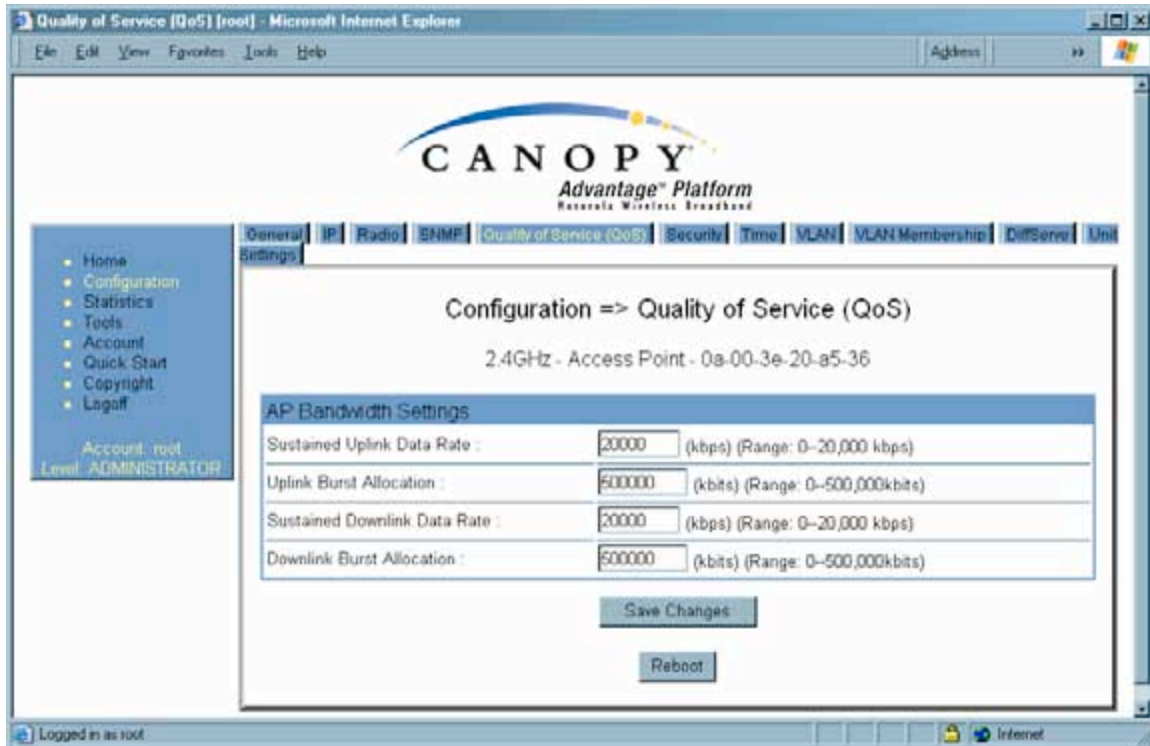
When you click this button

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



### 18.1.5 Quality of Service (QoS) Tab of the AP

An example of the Quality of Service (QoS) tab of the AP is displayed in [Figure 79](#).



**Figure 79: Quality of Service (QoS) tab of AP, example**

In the Quality of Service (QoS) tab, you may set AP bandwidth parameters as follows.

#### **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 84
- [Interaction of Burst Allocation and Sustained Data Rate Settings](#) on Page 86
- [Setting the Configuration Source](#) on Page 292.

#### **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 84
- [Interaction of Burst Allocation and Sustained Data Rate Settings](#) on Page 86
- [Setting the Configuration Source](#) on Page 292.

**Sustained Downlink Data Rate**

Specify the rate at which the AP should be 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 84
- [Interaction of Burst Allocation and Sustained Data Rate Settings](#) on Page 86
- [Setting the Configuration Source](#) on Page 292.

**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 84
- [Interaction of Burst Allocation and Sustained Data Rate Settings](#) on Page 86
- [Setting the Configuration Source](#) on Page 292.

The Quality of Server (QoS) 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.

### 18.1.6 Security Tab of the AP

An example of the Security tab of the AP is displayed in [Figure 80](#).



Figure 80: Security tab of AP, example

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

#### Authentication Mode

If the AP has authentication capability, then you can use this field to select from among the following authentication modes:

- **Authentication Disabled**—the AP requires no SMs to authenticate.

- **Authentication Required**—the AP requires any SM that attempts registration to be authenticated in BAM or Prizm before registration.

If the AP *does not* have authentication capability, then this parameter displays **Authentication Not Available**.

#### **Authentication Server 1 to 3**

If either BAM or the BAM subsystem in Prizm is implemented and the AP has authentication capability, enter the IP address of one or more BAM servers that perform authentication for SMs registered to this AP. Enter these in order of primary, secondary, then tertiary.

#### **Encryption**

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

- **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.

#### **Encrypt Downlink Broadcast**

When **Encryption Enabled** is selected in the **Airlink Security** parameter (described above) and **Enable** is selected in the **Encrypt Downlink Broadcast** parameter, the AP encrypts downlink broadcast packets as

- DES where the AP is DES capable.
- AES where the AP is AES capable.

For more information about the Encrypt Downlink Broadcast feature, see [Encrypting Downlink Broadcasts](#) on Page 378.

#### **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, 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 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.

The Security tab of the AP 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.

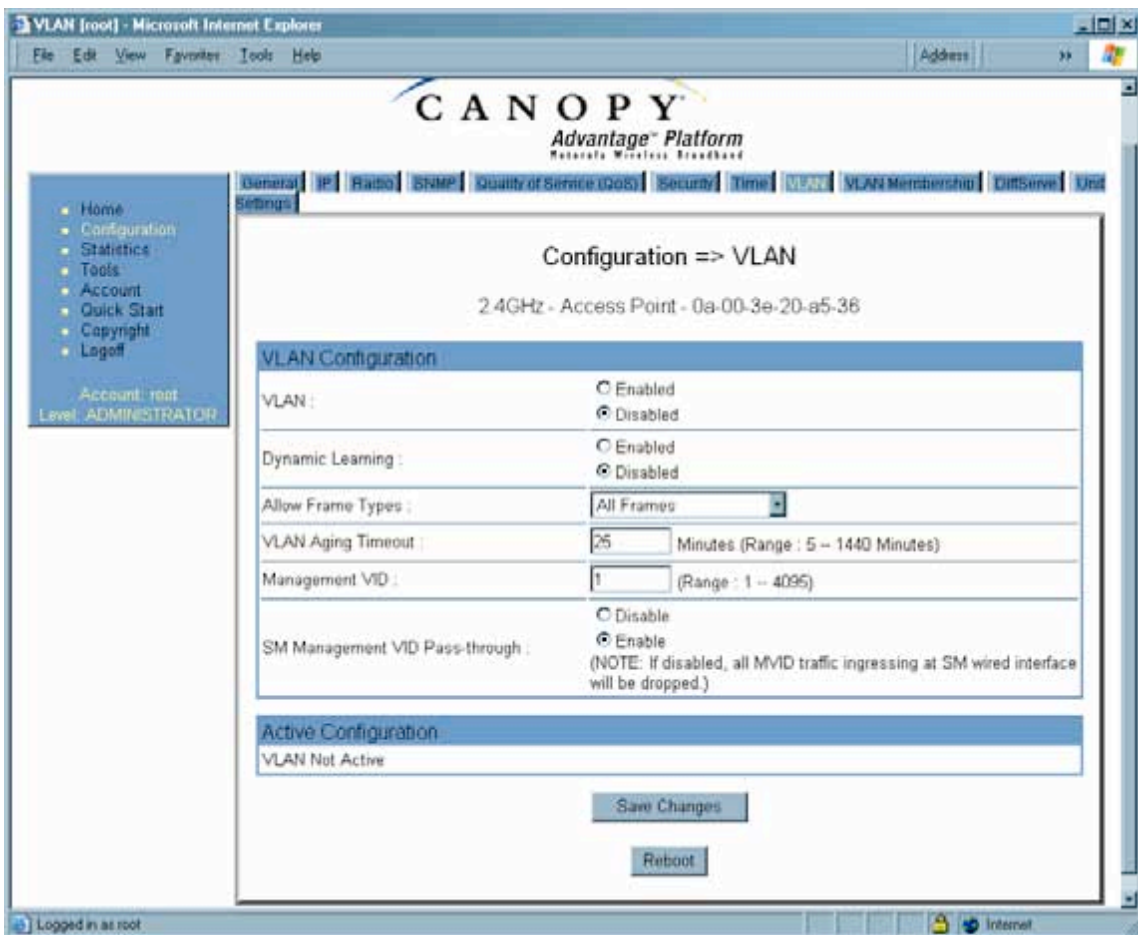
### Reboot

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.

## 18.1.7 VLAN Tab of the AP

An example of the AP VLAN tab is displayed in [Figure 81](#).



**Figure 81: VLAN tab of AP, example**

In the VLAN tab of the AP, you may set the following parameters.

### VLAN

Specify whether VLAN functionality for the AP and all linked SMs should (**Enabled**) or should not (**Disabled**) be allowed. The default value is **Disabled**.

### Dynamic Learning

Specify whether the AP should (**Enabled**) or should not (**Disabled**) add the VLAN IDs (VIDs) of upstream frames to the VID table. (The AP passes frames with VIDs that are stored in the table both upstream and downstream.) The default value is **Enabled**.

### Allow Frame Types

Select the type of arriving frames that the AP should tag, using the VID that is stored in the **Untagged Ingress VID** parameter. The default value is **All Frames**.

### VLAN Aging Timeout

Specify how long the AP should keep dynamically learned VIDs. The range of values is 5 to 1440 (minutes). The default value is **25** (minutes).



**NOTE:**

VIDs that you enter for the **Management VID** and **VLAN Membership** parameters do not time out.

### Management VID

Enter the VID that the operator wishes to use to communicate with the module manager. The range of values is 1 to 4095. The default value is **1**.

### SM Management VID Pass-through

Specify whether to allow the SM (**Enable**) or the AP (**Disable**) to control the VLAN settings of this SM. The default value is **Enable**.



**CAUTION!**

Do not set this parameter to **Enable** where both

- a BAM release earlier than 2.1 is implemented.
- the **Configuration Source** parameter in the AP is set to **BAM**.

This combination causes the SMs to become unmanageable, until you gain direct access with an override plug and remove this combination from the AP configuration.

### 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.

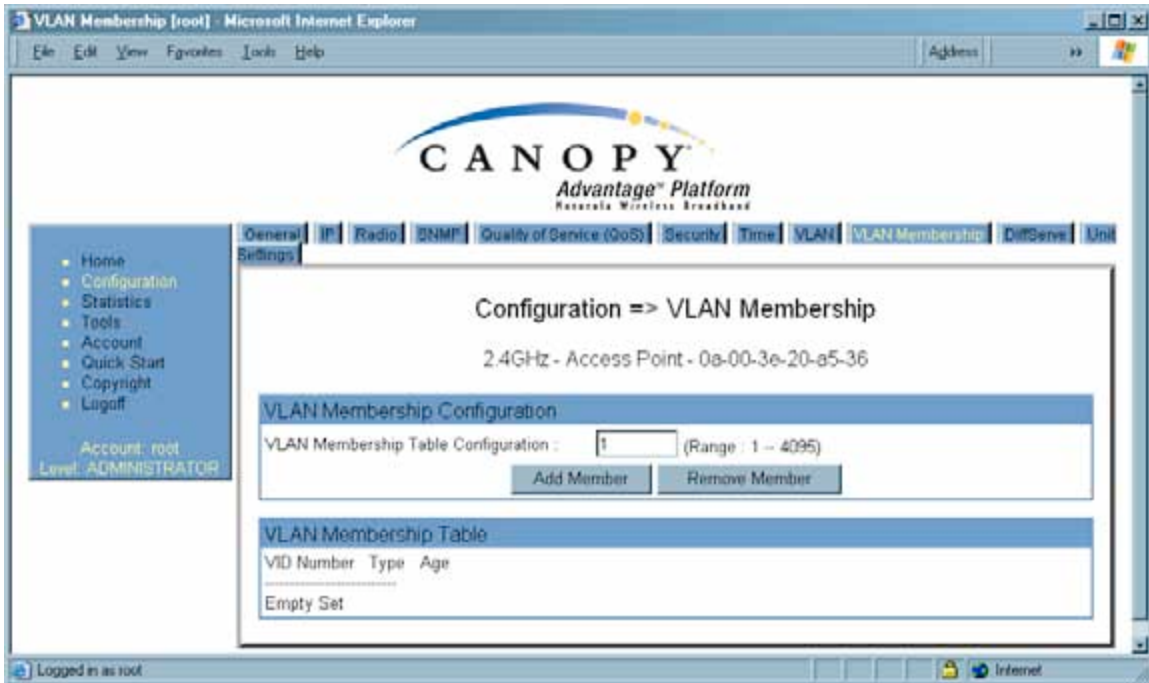
### Reboot

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.

### 18.1.8 VLAN Membership Tab of the AP

An example of the VLAN Membership tab of the AP is displayed in [Figure 82](#).



**Figure 82: VLAN Membership tab of AP, example**

You may set the VLAN Membership tab parameter as follows.

#### **VLAN Membership Table Configuration**

For each VLAN in which you want the AP to be a member, enter the VLAN ID and then click the **Add Member** button. Similarly, for any VLAN in which you want the AP to no longer be a member, enter the VLAN ID and then click the **Remove Member** button.

### 18.1.9 DiffServe Tab of the AP

An example of the DiffServe tab of the AP is displayed in Figure 83.

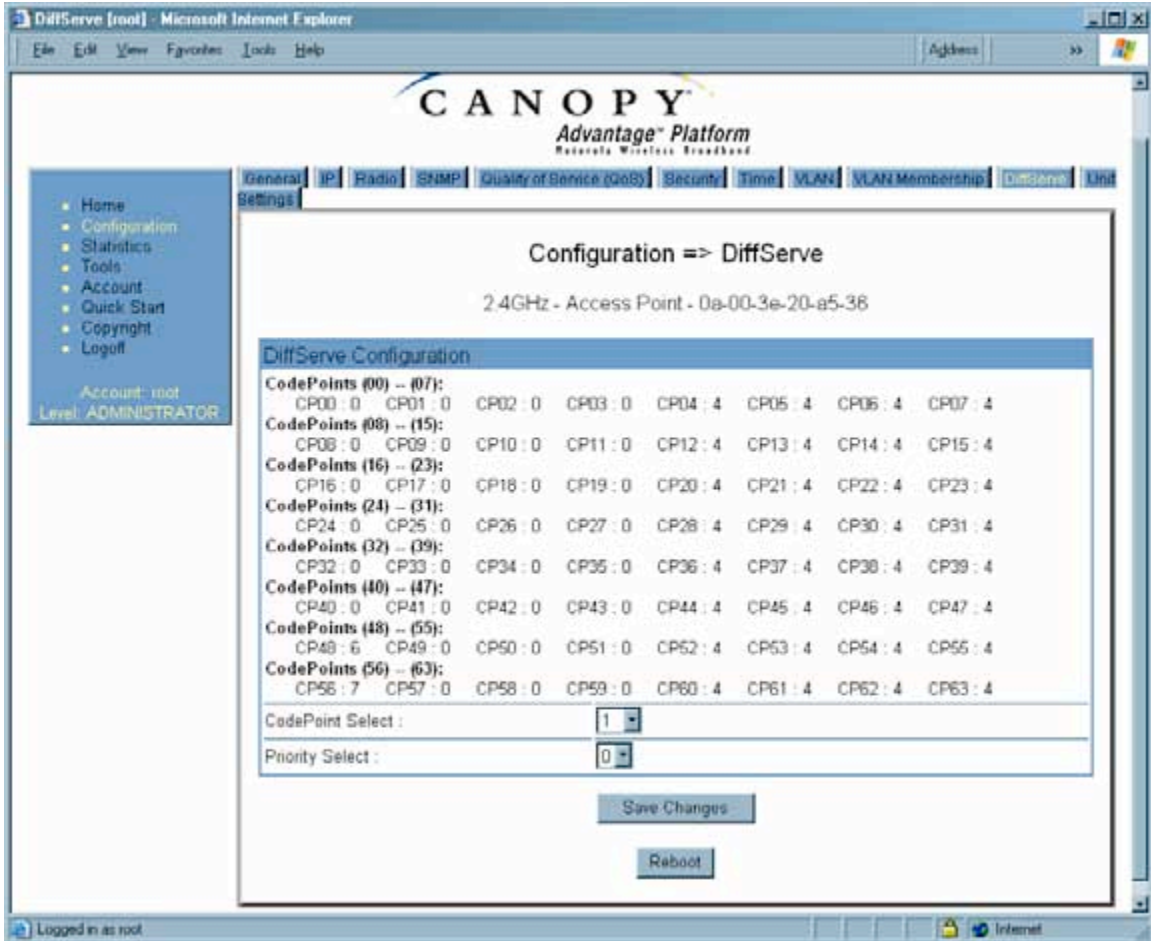


Figure 83: DiffServe tab of AP, example



You may set the following DiffServe tab parameters.

**CodePoint 1  
through  
CodePoint 47**

The default priority value for each settable CodePoint is shown in [Figure 113](#). 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).

**CodePoint 49  
through  
CodePoint 55**

**CodePoint 57  
through  
CodePoint 63**

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 [87](#).

The DiffServe 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.

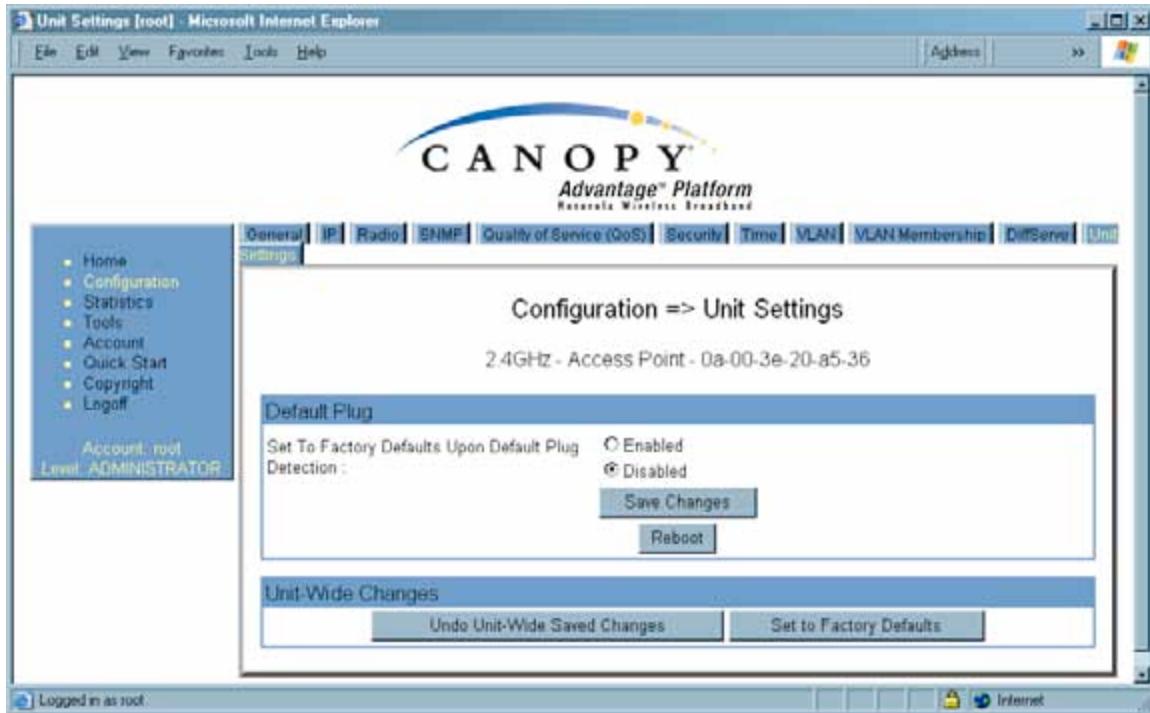
**Reboot**

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.

### 18.1.10 Unit Settings Tab of the AP

An example of the Unit Settings tab of the AP is shown in [Figure 84](#).



**Figure 84: Unit Settings tab of AP, example**

The Unit Settings tab of the AP contains an option for how the AP 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 373.

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**

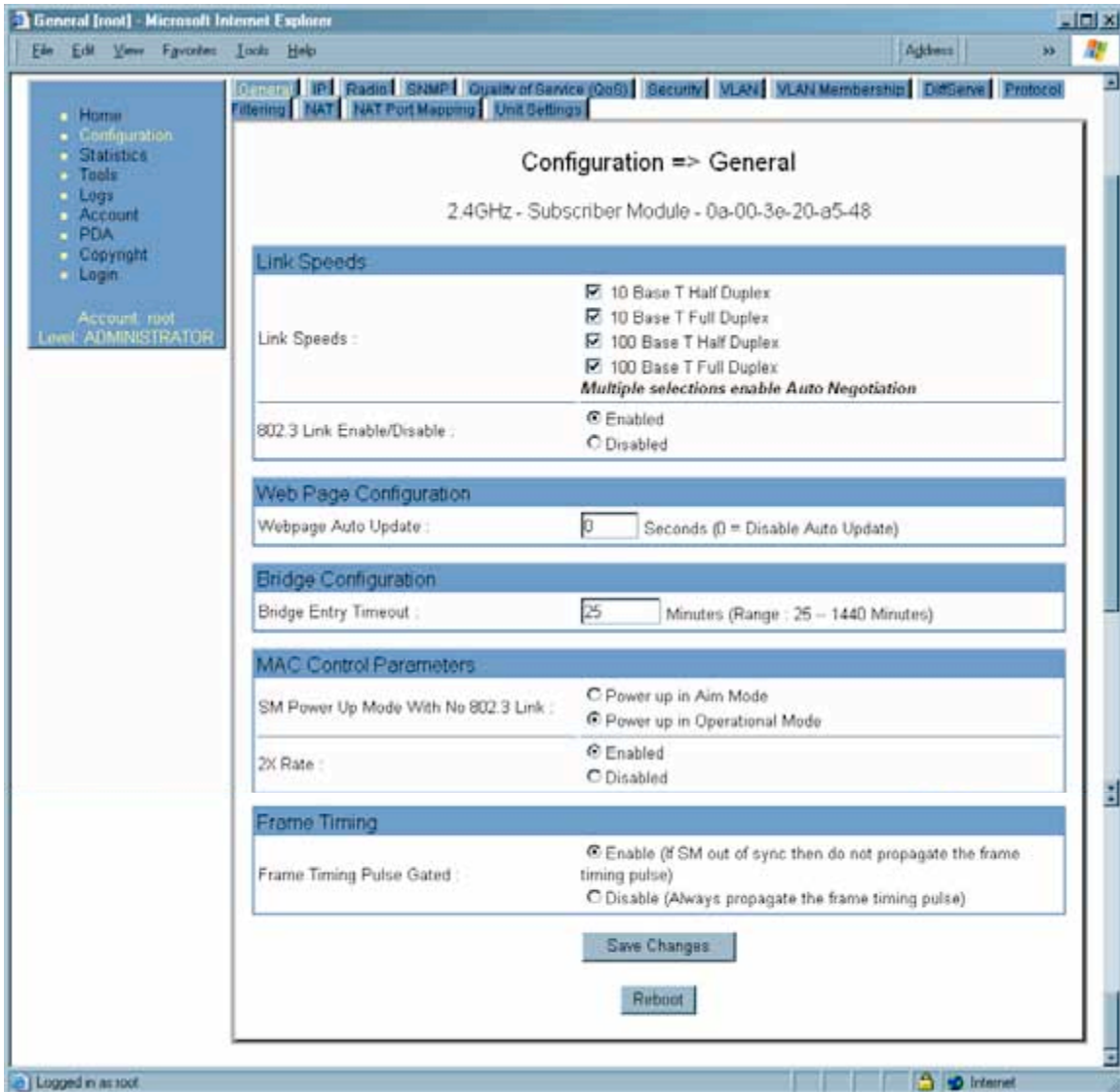
When you click this button, *all configurable parameters on all tabs* are reset to the factory settings.

**18.2 CONFIGURING AN SM FOR THE DESTINATION**

If an ADMINISTRATOR-level password has been set in the SM, you must log into the module before you can configure its parameters. See [Managing Module Access by Passwords](#) on Page 371.

### 18.2.1 General Tab of the SM

An example of a General tab in the SM is displayed in [Figure 85](#).



**Figure 85: General tab of SM, example**

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

#### 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.

### 802.3 Link Enable/Disable

Specify whether to enable or disable Ethernet/802.3 connectivity on the wired port of the SM. This parameter has no effect on the wireless link. When you select **Enable**, this feature allows traffic on the Ethernet/802.3 port. This is the factory default state of the port. When you select **Disable**, this feature prevents traffic on the port. Typical cases of when you may want to select **Disable** include:

- The subscriber is delinquent with payment(s).
- You suspect that the subscriber is sending or flooding undesired broadcast packets into the network, such as when
  - a virus is present in the subscriber's computing device.
  - the subscriber's home router is improperly configured.

### 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 AP encounters no activity with the SM (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.

### SM Power Up Mode With No 802.3 Link

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

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

### 2X Rate

Disable this parameter to facilitate initial aiming from the destination. Then see [2X Operation](#) on Page 89.

**Frame Timing Pulse Gated**

If this SM extends the sync pulse to a BH master or an AP, select either

- **Enable**—If this SM loses sync from the AP, then *do not* propagate a sync pulse to the BH timing master or other AP. This setting prevents interference in the event that the SM loses sync.
- **Disable**—If this SM loses sync from the AP, then propagate the sync pulse to the BH timing master or other AP.

See [Wiring to Extend Network Sync](#) on Page 367.

The General 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.

**18.2.2 NAT and IP Tabs of the SM with NAT Disabled**

An example of the NAT tab in an SM with NAT disabled is displayed in [Figure 86](#).

Configuration => NAT  
5.7GHz - Subscriber Module - 0s-00-3e-f0-08-09

**NAT Enable**  
NAT Enable/Disable :  Enabled  
 Disabled

**NAT Private Network Interface Configuration**  
IP Address : xxx.xxx.xxx.1  
Subnet Mask : 255.255.255.xxx

**DMZ Host Interface Configuration**  
IP Address : xxx.xxx.xxx.50  
DMZ Enable :  Enabled  
 Disabled

**NAT Public Network Interface Configuration**  
IP Address : 0.0.0.0  
Subnet Mask : 255.255.255.0  
Gateway IP Address : 0.0.0.0

**DHCP Server Network Interface Configuration**  
DHCP Start IP : xxx.xxx.xxx.2  
Number of IP's to Lease : 50

**Radio Public Network Interface Configuration**  
IP Address : 10.40.12.104  
Interface Enable/Disable :  Enabled  
 Disabled  
Subnet Mask : 255.255.0.0  
Gateway IP Address : 10.40.255.254  
DHCP state :  Enabled  
 Disabled

**Generic NAT Parameters**  
ARP Cache Timeout : 30 Minutes (Range : 1 - 30)  
TCP Session Garbage Timeout : 1440 Minutes (Range : 4 - 1440)  
UDP Session Garbage Timeout : 4 Minutes (Range : 1 - 1440)

**DHCP Generic Parameters**  
DHCP Client Enable/Disable :  Enabled  
 Disabled  
DHCP Server Enable/Disable :  Enabled  
 Disabled  
DHCP Server Lease Timeout : 30 Days (Range : 1 - 30)

**DNS Server Parameters**  
DNS IP Address :  Obtain Automatically  
 Set Manually  
Preferred DNS IP Address : 0.0.0.0  
Alternate DNS IP Address : 0.0.0.0

Save Changes  
Reboot

Figure 86: NAT tab of SM with NAT disabled, example

This implementation is illustrated in Figure 40 on Page 157. In the NAT tab of an SM with NAT disabled, you may set the following parameters.

**NAT Enable/Disable**

This parameter enables or disabled the Network Address Translation (NAT) feature for the SM. NAT isolates devices connected to the Ethernet/wired side of an SM from being seen directly from the wireless side of the SM. With NAT enabled, the SM has an IP address for transport traffic separate from its address for management, terminates transport traffic, and allows you to assign a range of IP addresses to devices that are connected to the Ethernet/wired side of the SM. For further information, see [Network Address Translation \(NAT\)](#) on Page 156 and [NAT and IP Tabs of the SM with NAT Enabled](#) on Page 268.

**NAT Private Network Interface Configuration, IP Address**

This parameter is not configurable when NAT is disabled.

**NAT Private Network Interface Configuration, Subnet Mask**

This parameter is not configurable when NAT is disabled.

**DMZ Host Interface Configuration, IP Address**

This parameter is not configurable when NAT is disabled.

**DMZ Enable**

This parameter is not configurable when NAT is disabled.

**NAT Public Network Interface Configuration, IP Address**

This field displays the IP address for the SM. DHCP Server *will not* automatically assign this address when NAT is disabled.

**NAT Public Network Interface Configuration, Subnet Mask**

This field displays the subnet mask for the SM. DHCP Server *will not* automatically assign this address when NAT is disabled.

**NAT Public Network Interface Configuration, Gateway IP Address**

This field displays the gateway IP address for the SM. DHCP Server *will not* automatically assign this address when NAT is disabled.

**DHCP Start IP**

This parameter is not configurable when NAT is disabled.

**Number of IPs to Lease**

This parameter is not configurable when NAT is disabled.

**Radio Public Network Interface Configuration, IP Address**

This parameter is not configurable when NAT is disabled.

**Radio Public Network Interface Configuration, Interface Enable/Disable**

This parameter is not configurable when NAT is disabled.

**Radio Public Network Interface Configuration, Subnet Mask**

This parameter is not configurable when NAT is disabled.

**Radio Public Network Interface Configuration, Gateway IP Address**

This parameter is not configurable when NAT is disabled.



**Radio Public Network Interface Configuration, DHCP State**

This parameter is not configurable when NAT is disabled.

**ARP Cache Timeout**

If a router upstream has an ARP cache of longer duration (as some use 30 minutes), enter a value of longer duration than the router ARP cache. The default value of this field is 20 minutes.

**TCP Session Garbage Timeout**

Where a large network exists behind the SM, you can set this parameter to lower than the default value of 1440 minutes (24 hours). This action makes additional resources available for greater traffic than the default value accommodates.

**UDP Session Garbage Timeout**

You may adjust this parameter in the range of 1 to 1440 minutes, based on network performance. The default value of this parameter is 4 minutes.

**DHCP Client Enable/Disable**

This parameter is not configurable when NAT is disabled.

**DHCP Server Enable/Disable**

This parameter is not configurable when NAT is disabled.

**DHCP Server Lease Timeout**

This parameter is not configurable when NAT is disabled.

**DNS IP Address**

This parameter is not configurable when NAT is disabled.

**Preferred DNS IP Address**

This parameter is not configurable when NAT is disabled.

**Alternate DNS IP Address**

This parameter is not configurable when NAT is disabled.

The NAT tab also contains the following buttons.

**Save Changes**

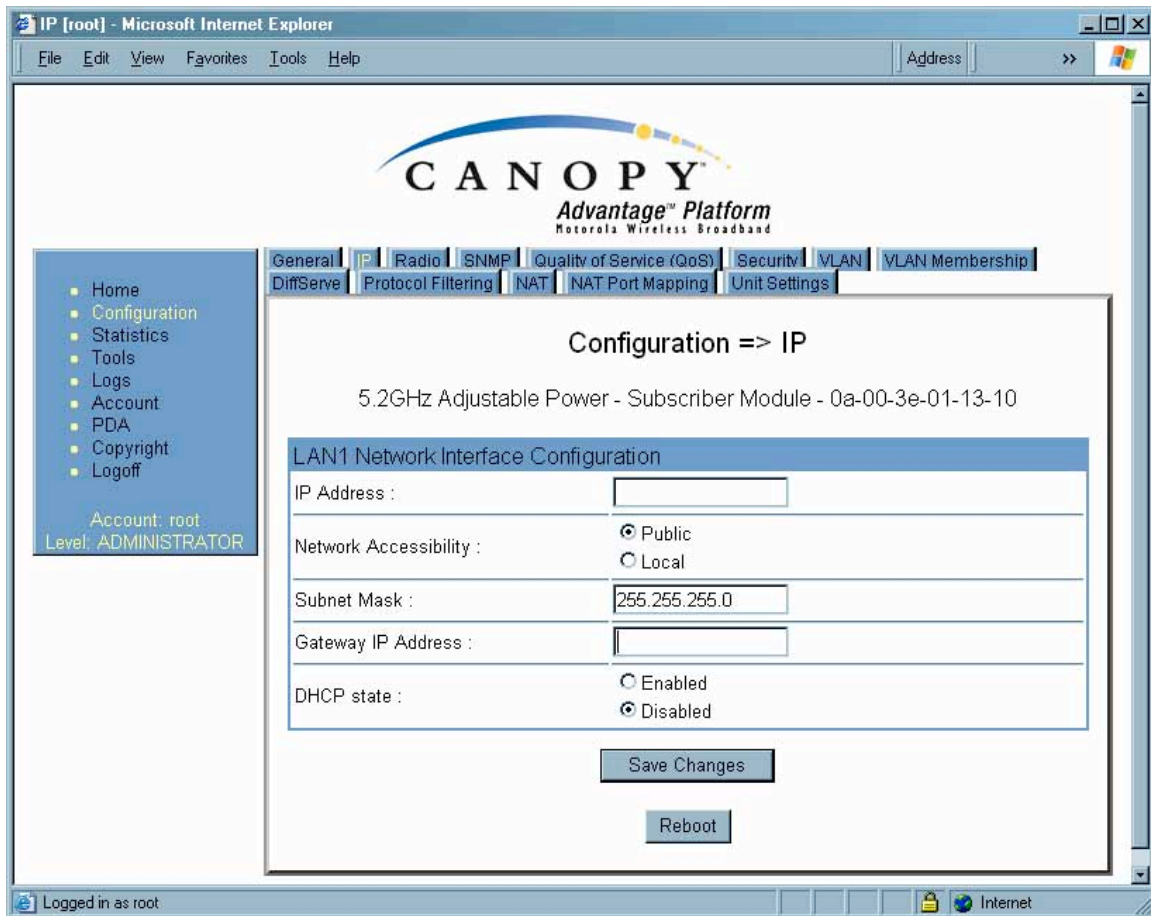
When you click this button, any changes that you made on all tabs are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

**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.

An example of the IP tab in an SM with NAT disabled is displayed in [Figure 87](#).



**Figure 87: IP tab of SM with NAT disabled, example**

This implementation is illustrated in [Figure 40](#) on [Page 157](#). In the IP tab of an SM with NAT disabled, 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 SM. (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 375](#).



#### **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, Network Accessibility**

Specify whether the IP address of the SM should be visible to only a device connected to the SM by Ethernet (**Local**) or should be visible to the AP as well (**Public**).

**LAN1 Network Interface Configuration, Subnet Mask**

Enter an appropriate subnet mask for the SM 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 SM 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.

In this tab, DHCP State is settable only if the **Network Accessibility** parameter in the IP tab is set to **Public**. This parameter is also settable in the NAT tab of the Configuration web page, but only when NAT is enabled.

The IP 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.

### 18.2.3 NAT and IP Tabs of the SM with NAT Enabled

An example of the NAT tab in an SM with NAT enabled is displayed in [Figure 88](#).

**Configuration => NAT**  
5.7GHz - Subscriber Module - Da-00-3e-f0-09-c7

**NAT Enable**  
NAT Enable/Disable:  Enabled  Disabled

**NAT Private Network Interface Configuration**  
IP Address: 169.254.1.1  
Subnet Mask: 255.255.255.0

**DMZ Host Interface Configuration**  
IP Address: 169.254.1.52  
DMZ Enable:  Enabled  Disabled

**NAT Public Network Interface Configuration**  
IP Address: 0.0.0.0  
Subnet Mask: 255.255.255.0  
Gateway IP Address: 0.0.0.0

**DHCP Server Network Interface Configuration**  
DHCP Start IP: 169.254.1.2  
Number of IP's to Lease: 50

**Radio Public Network Interface Configuration**  
IP Address: 10.40.12.112  
Interface Enable/Disable:  Enabled  Disabled  
Subnet Mask: 255.255.0.0  
Gateway IP Address: 10.40.255.254  
DHCP state:  Enabled  Disabled

**Generic NAT Parameters**  
ARP Cache Timeout: 20 Minutes (Range: 1 - 30)  
TCP Session Garbage Timeout: 120 Minutes (Range: 4 - 1440)  
UDP Session Garbage Timeout: 5 Minutes (Range: 1 - 1440)

**DHCP Generic Parameters**  
DHCP Client Enable/Disable:  Enabled  Disabled  
DHCP Server Enable/Disable:  Enabled  Disabled  
DHCP Server Lease Timeout: 30 Days (Range: 1 - 30)

**DNS Server Parameters**  
DNS IP Address:  Obtain Automatically  Set Manually  
Preferred DNS IP Address: 0.0.0.0  
Alternate DNS IP Address: 0.0.0.0

Save Changes  
Reboot

**Figure 88: NAT tab of SM with NAT enabled, example**

In the NAT tab of an SM with NAT enabled, you may set the following parameters.

**NAT Enable/Disable**

This parameter enables or disabled the Network Address Translation (NAT) feature for the SM. NAT isolates devices connected to the Ethernet/wired side of an SM from being seen directly from the wireless side of the SM. With NAT enabled, the SM has an IP address for transport traffic separate from its address for management, terminates transport traffic, and allows you to assign a range of IP addresses to devices that are connected to the Ethernet/wired side of the SM. For further information, see [Network Address Translation \(NAT\)](#) on Page 156 and [NAT and IP Tabs of the SM with NAT Enabled](#) on Page 268.

**NAT Private Network Interface Configuration, IP Address**

Assign an IP address for SM management through Ethernet access to the SM. Set only the first three bytes. The last byte is permanently set to 1. This address becomes the base for the range of DHCP-assigned addresses.

**NAT Private Network Interface Configuration, Subnet Mask**

Assign a subnet mask of 255.255.255.0 or a more restrictive subnet mask. Set only the last byte of this subnet mask. Each of the first three bytes is permanently set to 255.

**DMZ Host Interface Configuration, IP Address**

If you will be enabling DMZ in the next parameter, set the last byte of the DMZ host IP address to use for this SM when DMZ is enabled. Only one such address is allowed. The first three bytes are identical to those of the NAT private IP address. Ensure that the device that should receive network traffic behind this SM is assigned this address. The system provides a warning if you enter an address within the range that DHCP can assign.

**DMZ Enable**

Either enable or disable DMZ for this SM. See [DMZ](#) on Page 156.

**NAT Public Network Interface Configuration, IP Address**

This field displays the IP address of the SM. If DHCP Client is enabled, then the DHCP server automatically assigns this address.

**NAT Public Network Interface Configuration, Subnet Mask**

This field displays the subnet mask of the SM. If DHCP Client is enabled, then the DHCP server automatically assigns this subnet mask.

**NAT Public Network Interface Configuration, Gateway IP Address**

This field displays the gateway IP address for the SM. If DHCP Client is enabled, then the DHCP server automatically assigns this gateway IP address.

**DHCP Start IP**

If you will be enabling DHCP Server below, set the last byte of the starting IP address that the DHCP server will assign. The first three bytes are identical to those of the NAT private IP address.

**Number of IPs to Lease**

Enter how many IP addresses the DHCP server is allowed to assign. The default value is 50 addresses.

**Radio Public Network Interface Configuration, IP Address**

If DHCP Client is enabled, then the DHCP server automatically assigns this address. Otherwise, assign the IP address for over-the-air management of the SM when the radio public interface is enabled in the next parameter.

**Radio Public Network Interface Configuration, Interface Enable/Disable**

If you want over-the-air management capability for the SM, select **Enabled**. If you want to limit management of the SM to its Ethernet interface, select **Disabled**.

**Radio Public Network Interface Configuration, Subnet Mask**

If DHCP Client is enabled, then the DHCP server automatically assigns this subnet mask. Otherwise, assign the subnet mask for over-the-air management of the SM when the radio public interface is enabled.

**Radio Public Network Interface Configuration, Gateway IP Address**

If DHCP Client is enabled, then the DHCP server automatically assigns this gateway IP address. Otherwise, assign the gateway IP address for over-the-air management of the SM when the radio public network interface is enabled.

**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.

**Radio Public 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.

**ARP Cache Timeout**

If a router upstream has an ARP cache of longer duration (as some use 30 minutes), enter a value of longer duration than the router ARP cache. The default value of this field is 20 minutes.

**TCP Session Garbage Timeout**

Where a large network exists behind the SM, you can set this parameter to lower than the default value of 1440 minutes (24 hours). This action makes additional resources available for greater traffic than the default value accommodates. The default value of this parameter is 120 minutes.

**UDP Session Garbage Timeout**

You may adjust this parameter in the range of 1 to 1440 minutes, based on network performance. The default value of this parameter is 4 minutes.

### DHCP Client Enable/Disable

Select either

- **Enabled** to allow the network DHCP server to assign IP addresses, subnet masks, and gateway IP addresses to devices that are attached to the SM.
- **Disabled** to
  - disable DHCP server assignment of this address.
  - enable the operator to assign this address.

The implementation of NAT with DHCP client is illustrated in [Figure 42](#) on Page 159. The implementation of NAT with DHCP client and DHCP server is illustrated in [Figure 41](#) on Page 158. The implementation of NAT without DHCP is illustrated in [Figure 44](#) on Page 161.

### DHCP Server Enable/Disable

Select either

- **Enabled** to
  - allow this SM to assign IP addresses, subnet masks, and gateway IP addresses to attached devices.
  - assign a start address for DHCP.
  - designate how many IP addresses may be temporarily used (leased).
- **Disabled** to disallow the SM to assign addresses to attached devices.

The implementation of NAT with DHCP server is illustrated in [Figure 43](#) on Page 50. The implementation of NAT with DHCP client and DHCP server is illustrated in [Figure 41](#) on Page 158. The implementation of NAT without DHCP is illustrated in [Figure 44](#) on Page 161.

### DHCP Server Lease Timeout

Based on network performance, enter the number of days between when the DHCP server assigns an IP address and when that address expires. The range of values for this parameter is 1 to 30 days. The default value is 30 days.

### DNS IP Address

Select either

- **Obtain Automatically** to allow the system to set the IP address of the DNS server.
- **Set Manually** to enable yourself to set both a preferred and an alternate DNS IP address.

### Preferred DNS IP Address

Enter the preferred DNS IP address to use when the **DNS IP Address** parameter is set to **Set Manually**.

### Alternate DNS IP Address

Enter the DNS IP address to use when the **DNS IP Address** parameter is set to **Set Manually** and no response is received from the preferred DNS IP address.

The NAT tab also contains the following buttons.

### Save Changes

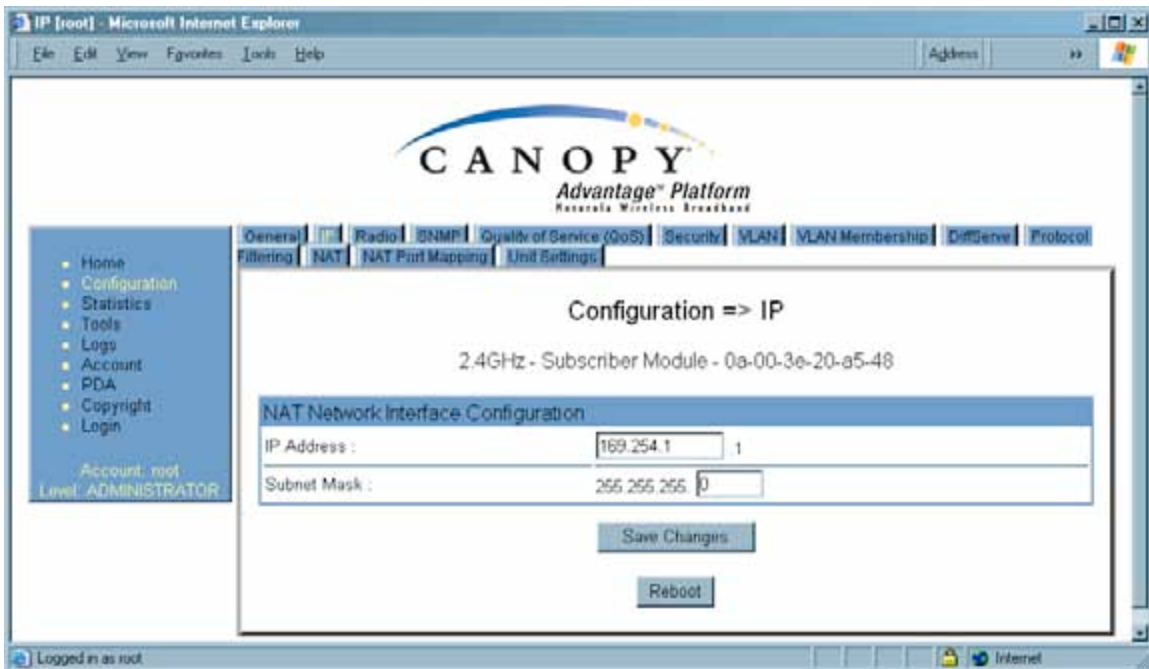
When you click this button, any changes that you made on all tabs are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

### 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.

An example of the IP tab in an SM with NAT enabled is displayed in [Figure 89](#).



**Figure 89: IP tab of SM with NAT enabled, example**

In the IP tab of an SM with NAT enabled, you may set the following parameters.

#### **NAT Network Interface Configuration, IP Address**

Assign an IP address for SM management through Ethernet access to the SM. Set only the first three bytes. The last byte is permanently set to 1. This address becomes the base for the range of DHCP-assigned addresses.

#### **NAT Network Interface Configuration, Subnet Mask**

Assign a subnet mask of 255.255.255.0 or a more restrictive subnet mask. Set only the last byte of this subnet mask. Each of the first three bytes is permanently set to 255.

The IP 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

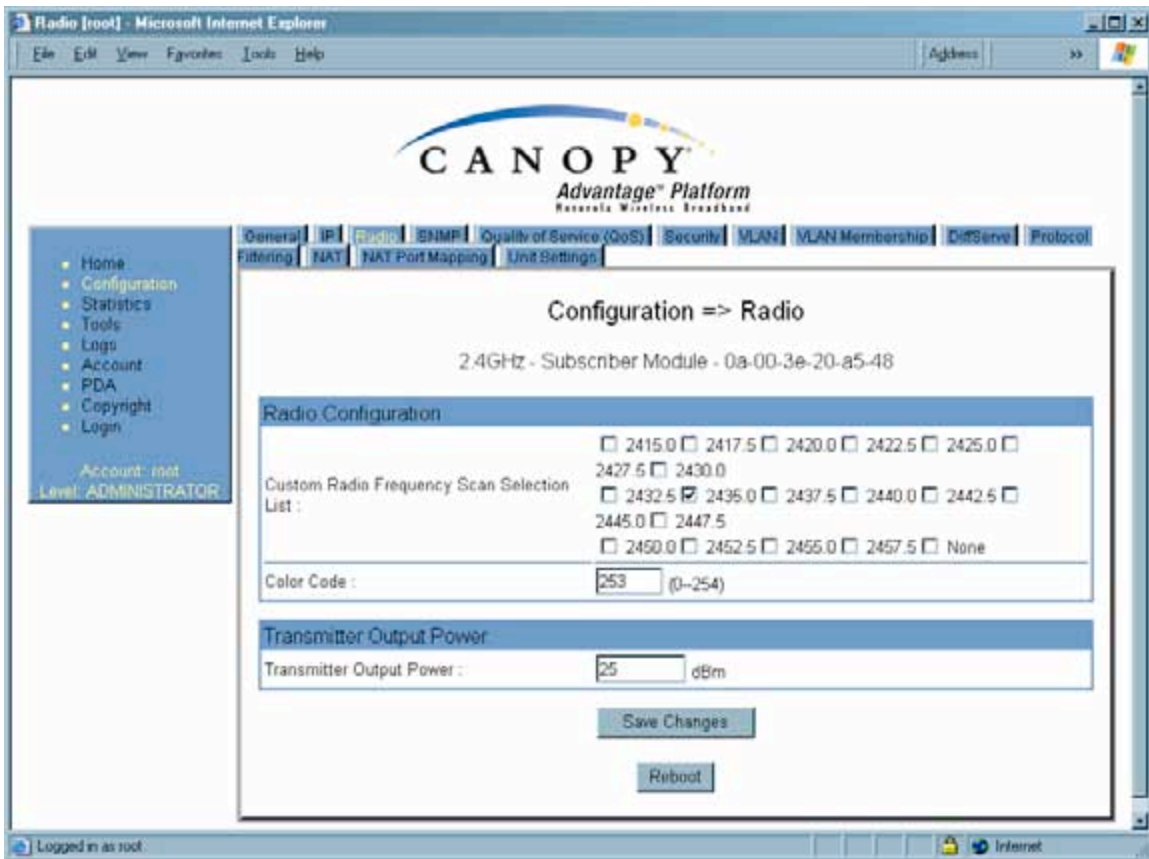
When you click this button

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

An example of the IP tab in an SM with NAT enabled is displayed in [Figure 89](#).

### 18.2.4 Radio Tab of the SM

An example of the Radio tab in the SM is displayed in [Figure 90](#).



**Figure 90: Radio tab of SM, example**

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

#### Custom Radio Frequency Scan Selection List

Check any frequency that you want the SM to scan for AP transmissions. The frequency *band* of the SM affects what channels you should select.

**IMPORTANT!**

In the 2.4-GHz frequency band, the SM can register to an AP that transmits on a frequency 2.5 MHz higher than the frequency that the SM 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 SM, 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 SM, this parameter displays only ISM frequencies. In a 5.7-GHz SM, this parameter displays both ISM and U-NII frequencies. If you select all frequencies that are listed in this field (default selections), then the SM scans for a signal on any channel. If you select only one, then the SM 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.

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**

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. 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.

**External Filters Delay**

This parameter is present in only 900-MHz modules and can have effect in only those that have interference mitigation filter(s). If this value is present, leave it set to **0**, regardless of whether the SM has an interference mitigation filter.

### 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 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.

## 18.2.5 SNMP Tab of the SM

An example of the SNMP tab in an SM is displayed in [Figure 91](#).

SNMP [root] - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address

General IP Radio **SNMP** Quality of Service (QoS) Security VLAN VLAN Membership DiffServ Protocol Filtering  
NAT Port Mapping Unit Settings

Configuration => SNMP

2.4GHz - Subscriber Module - 0a-00-3e-20-a5-48

**SNMP IP**

Community String : Canopy BOST

Accessing Subnet : 0.0.0.0 / 0

**Trap Addresses**

Trap Address 1 :

Trap Address 2 : 192.168.1.253

Trap Address 3 : 0.0.0.0

Trap Address 4 :

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 : 192.168.1.253

**Permissions**

Read Permissions :  Read Only  
 Read / Write

**Site Information**

Site Name : Camera Client

Site Contact : No Site Contact3

Site Location : No Site Location

Save Changes

Reboot

Logged in as root

Internet

**Figure 91: SNMP tab of SM, example**

In the SNMP tab of the SM, 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 SM. 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 SM. 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 SM, 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.”



#### **RECOMMENDATION:**

The subscriber can access the SM 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 to filter (block) SNMP requests. See [Filtering Protocols and Ports](#) on Page 376.

### 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.

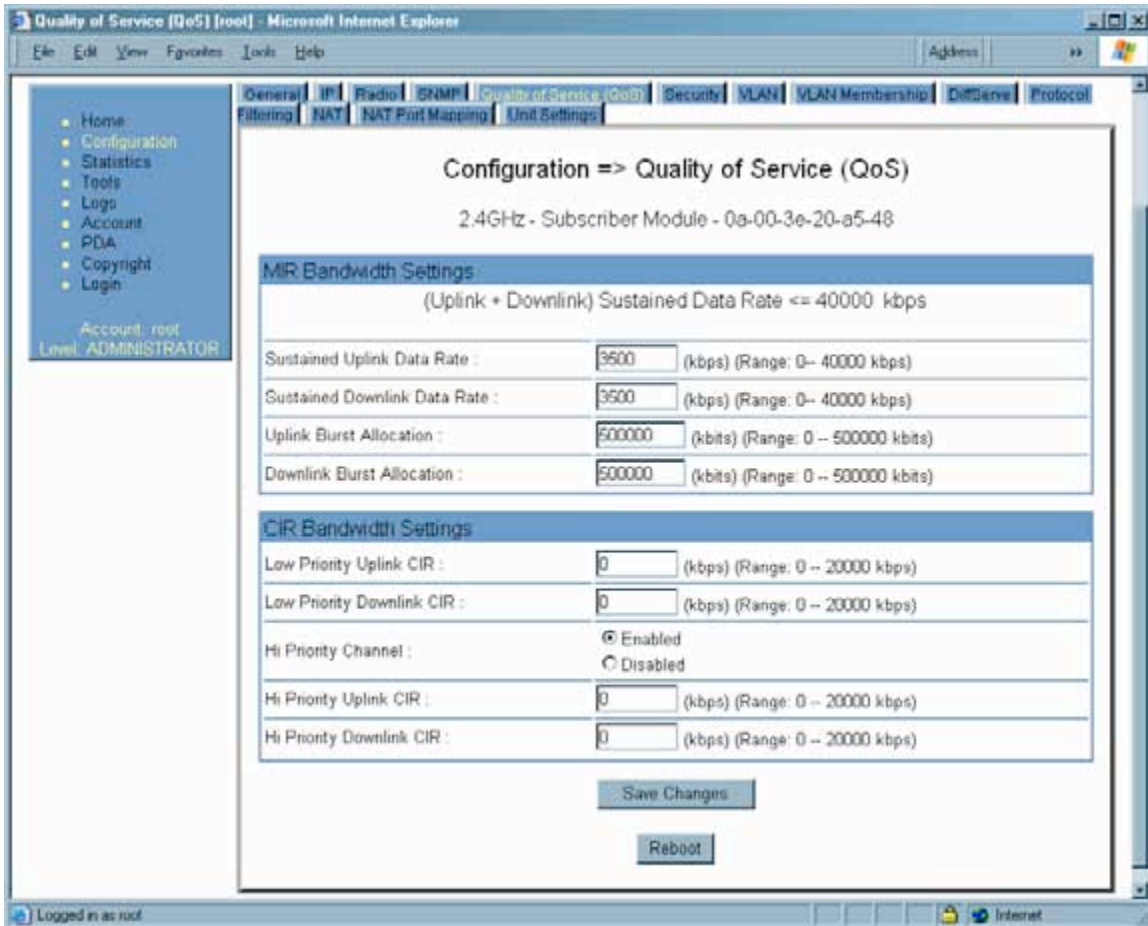
**Reboot**

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.

## 18.2.6 Quality of Service (QoS) Tab of the SM

An example of the Quality of Service (QoS) tab in the SM is displayed in [Figure 92](#).



**Figure 92: Quality of Service (QoS) tab of SM, example**

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

### 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 84
- [Interaction of Burst Allocation and Sustained Data Rate Settings](#) on Page 86
- [Setting the Configuration Source](#) on Page 292.

### Sustained Downlink Data Rate

Specify the rate at which the AP should be 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 84
- [Interaction of Burst Allocation and Sustained Data Rate Settings](#) on Page 86
- [Setting the Configuration Source](#) on Page 292.

**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 84
- [Interaction of Burst Allocation and Sustained Data Rate Settings](#) on Page 86
- [Setting the Configuration Source](#) on Page 292.

**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 84
- [Interaction of Burst Allocation and Sustained Data Rate Settings](#) on Page 86
- [Setting the Configuration Source](#) on Page 292.

**Low Priority Uplink CIR**

See

- [Committed Information Rate](#) on Page 86
- [Setting the Configuration Source](#) on Page 292.

**Low Priority Downlink CIR**

See

- [Committed Information Rate](#) on Page 86
- [Setting the Configuration Source](#) on Page 292.

**Hi Priority Channel**

See

- [High-priority Bandwidth](#) on Page 86
- [Setting the Configuration Source](#) on Page 292.

**Hi Priority Uplink CIR**

See

- [High-priority Bandwidth](#) on Page 86
- [Committed Information Rate](#) on Page 86
- [Setting the Configuration Source](#) on Page 292.

**Hi Priority Downlink CIR**

See

- [High-priority Bandwidth](#) on Page 86



- [Committed Information Rate](#) on Page 86
- [Setting the Configuration Source](#) on Page 292.

The Quality of Service (QoS) tab also provides the following buttons.

**Save Changes**

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

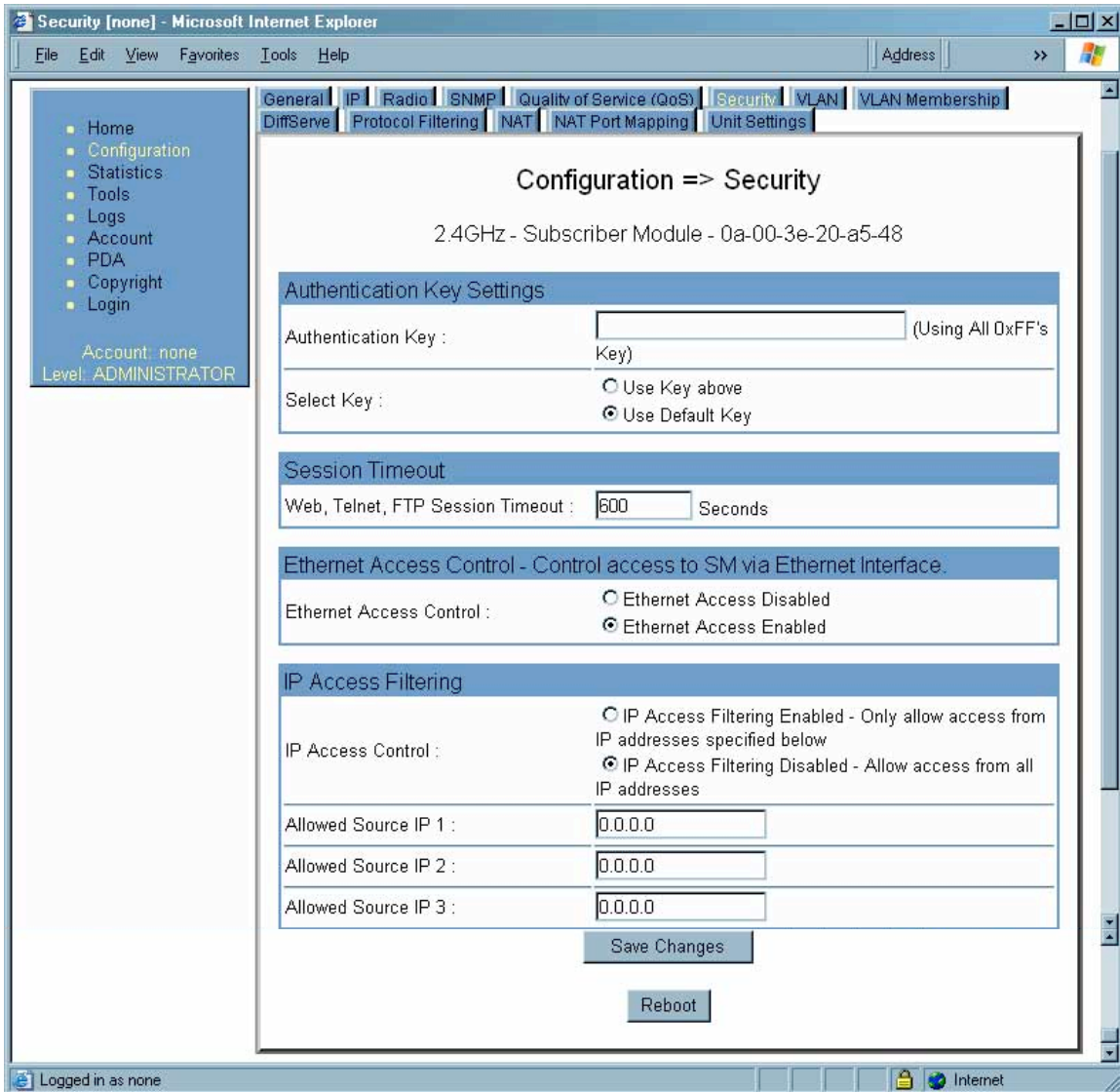
**Reboot**

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.

## 18.2.7 Security Tab of the SM

An example of the Security tab in an SM is displayed in [Figure 93](#).



**Figure 93: Security tab of SM, example**

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

### Authentication Key

Only if the AP to which this SM will register requires authentication, specify the key that the SM should 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 BAM or Prizm. See [Authentication Manager Capability](#) on Page 383.

The **Use Key above** selection specifies the 32-digit hexadecimal key that is permanently stored on both the SM and the BAM or Prizm database.



#### NOTE:

The SM and BAM or Prizm pad the key of any length by the addition of leading zeroes, and if the entered keys match, authentication attempts succeed. However, Canopy recommends that you enter 32 characters to achieve the maximal security from this feature.

### 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 Control

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, 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 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.

The Security tab of the SM 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.

## 18.2.8 VLAN Tab of the SM

An example of the VLAN tab in an SM is displayed in [Figure 94](#).

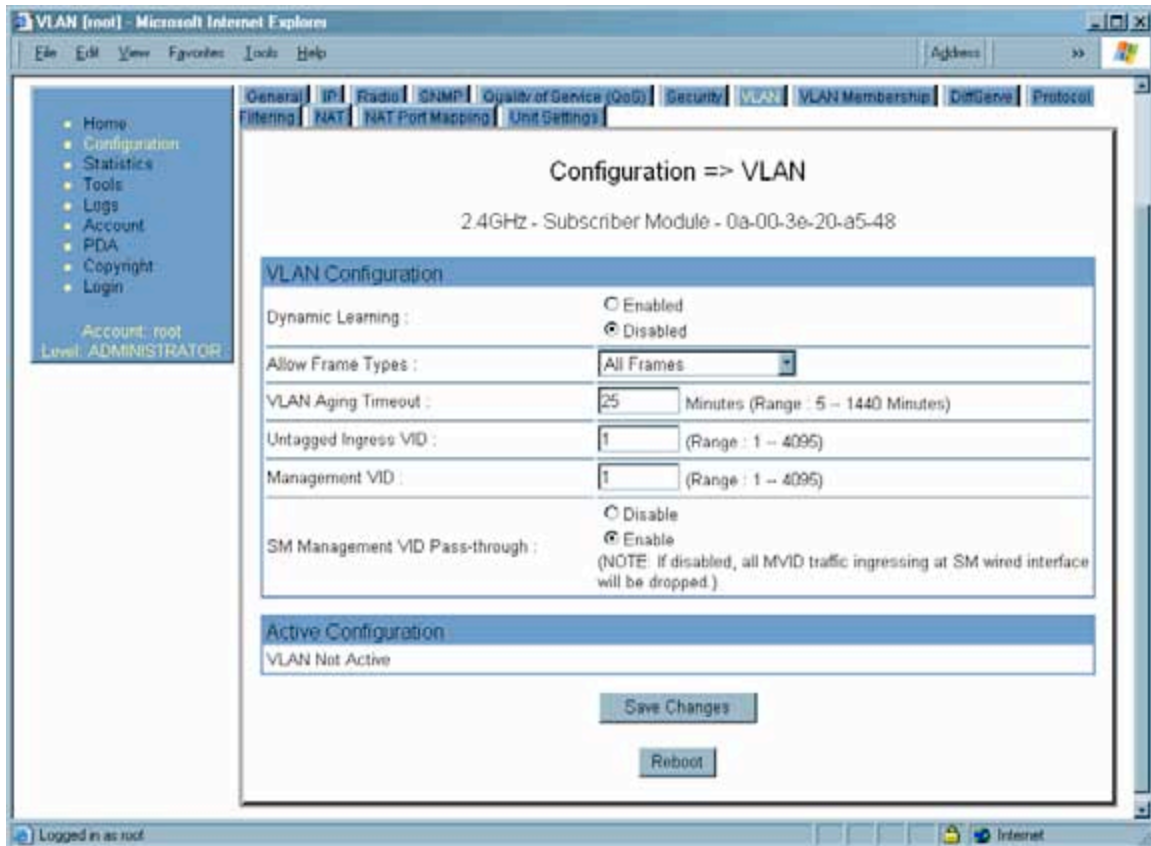


Figure 94: VLAN tab of SM, example

In the VLAN tab of an SM, you may set the following parameters.

### Dynamic Learning

Specify whether the SM should (**Enable**) or should not (**Disable**) add the VIDs of upstream frames (that enter the SM through the wired Ethernet interface) to the VID table. The default value is **Enable**.

### Allow Frame Types

Select the type of arriving frames that the SM should tag, using the VID that is stored in the **Untagged Ingress VID** parameter. The default value is **All Frames**.

### VLAN Aging Timeout

Specify how long the SM should keep dynamically learned VIDs. The range of values is 5 to 1440 (minutes). The default value is **25** (minutes).



**NOTE:**

VIDs that you enter for the **Untagged Ingress VID** and **Management VID** parameters do not time out.

### Untagged Ingress VID

Enter the VID that the SM(s) should use to tag frames that arrive at the SM(s) untagged. The range of values is 1 to 4095. The default value is **1**.

### Management VID

Enter the VID that the SM should share with the AP. The range of values is 1 to 4095. The default value is **1**.

### SM Management VID Pass-through

Specify whether to allow the SM (**Enable**) or the AP (**Disable**) to control the VLAN settings of this SM. The default value is **Enable**.

The VLAN 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.

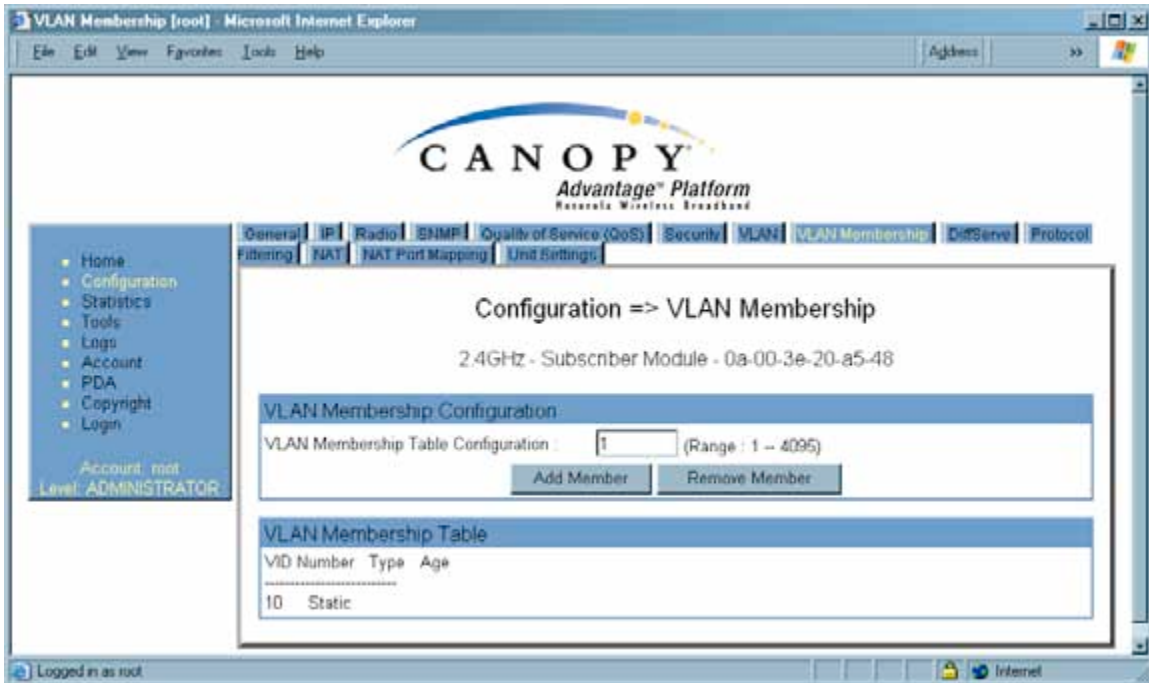
### Reboot

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.

### 18.2.9 VLAN Membership Tab of the SM

An example of the VLAN Membership tab in an SM is displayed in [Figure 95](#).



**Figure 95: VLAN Membership tab of SM, example**

In the VLAN Membership tab, you may set the following parameter.

#### **VLAN Membership Table Configuration**

For each VLAN in which you want the AP to be a member, enter the VLAN ID and then click the **Add Member** button. Similarly, for any VLAN in which you want the AP to no longer be a member, enter the VLAN ID and then click the **Remove Member** button.

### 18.2.10 DiffServe Tab of the SM

An example of the DiffServe tab in an SM is displayed in Figure 96.

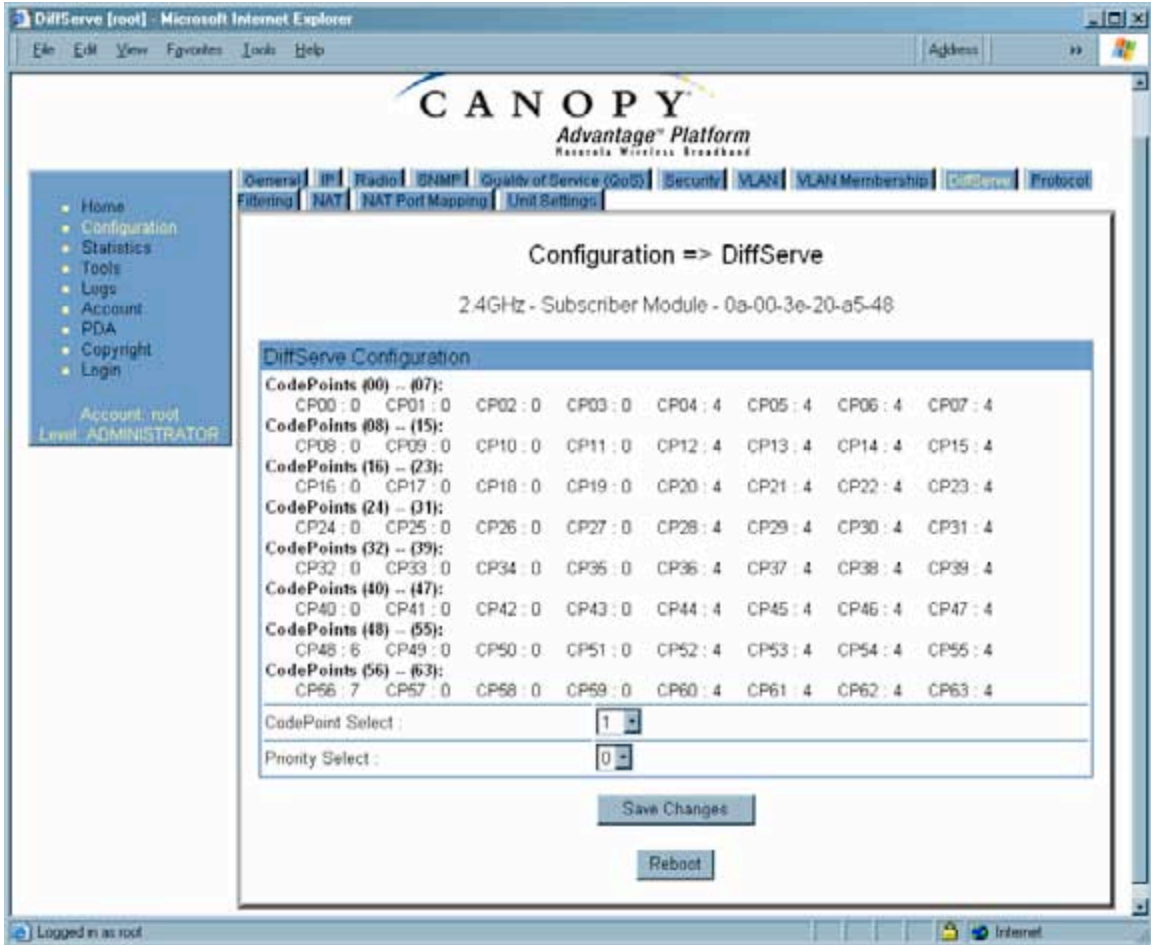


Figure 96: DiffServe tab of SM, example

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

**CodePoint 1  
through  
CodePoint 47**

The default priority value for each settable CodePoint is shown in [Figure 113](#). 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 49  
through  
CodePoint 55**

- **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).

**CodePoint 57  
through  
CodePoint 63**

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 87.

The DiffServe tab of the SM 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**

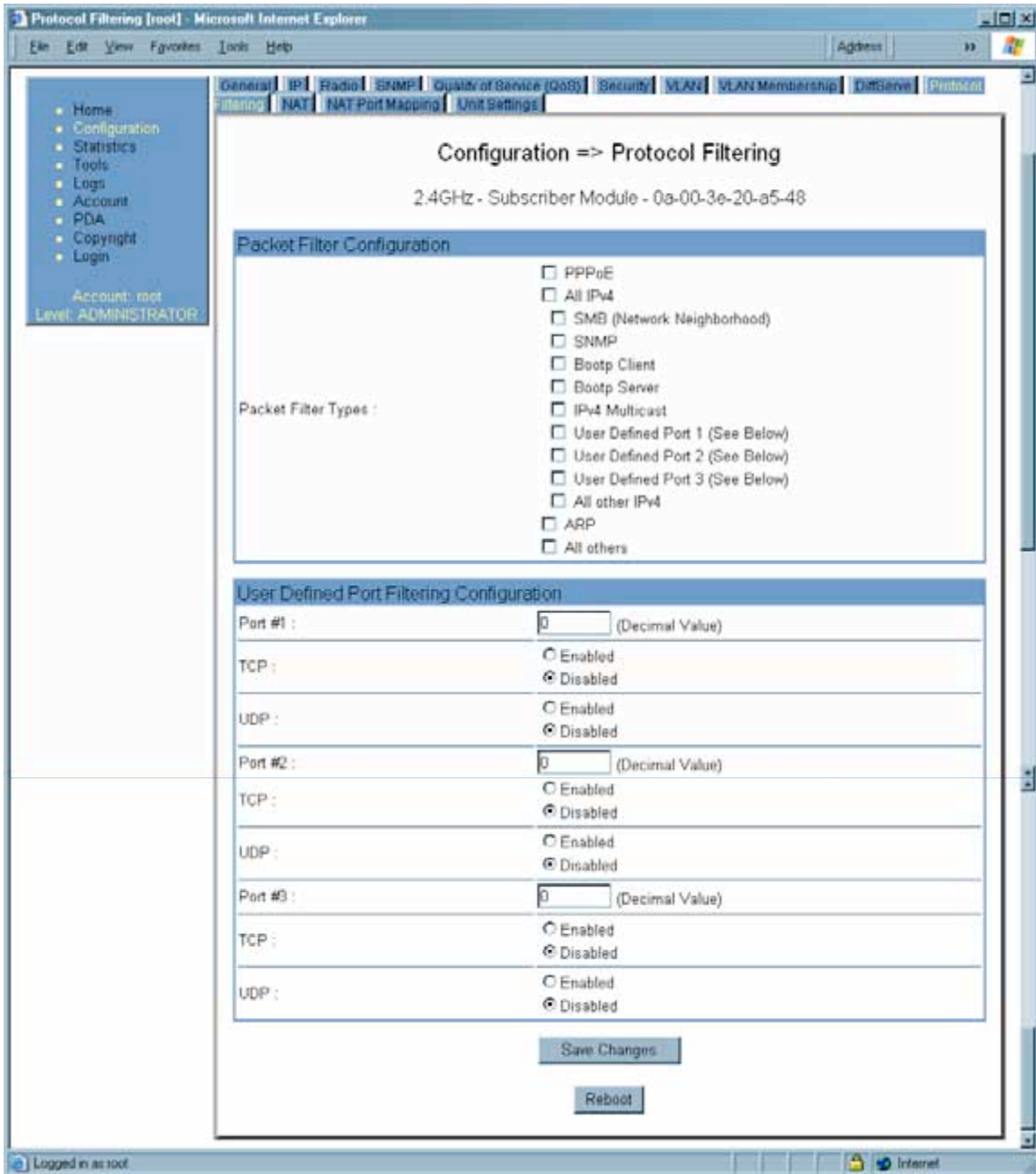
When you click this button

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



### 18.2.11 Protocol Filtering Tab of the SM

An example of the Protocol Filtering tab in an SM is displayed in [Figure 97](#).



**Figure 97: Protocol Filtering tab of SM, example**

In the Protocol Filtering tab of the SM, you may set the following parameters.

#### Packet Filter Types

For any box selected, the Protocol and Port Filtering feature blocks the associated protocol type. Examples are provided in [Protocol and Port Filtering with NAT Disabled](#) on [Page 376](#).

To filter packets in any of the user-defined ports, you must do all of the following:

- Check the box for **User Defined Port *n* (See Below)** in the **Packet Filter Types** section of this tab.
- In the **User Defined Port Filtering Configuration** section of this tab, both
  - provide a port number at **Port #*n***.
  - check **TCP**, **UDP**, or both.

### User Defined Port Filtering Configuration

You can specify ports for which to block subscriber access, regardless of whether NAT is enabled. For more information, see [Filtering Protocols and Ports](#) on Page 376.

## 18.2.12 NAT Port Mapping Tab of the SM

An example of the NAT Port Mapping tab in an SM is displayed in [Figure 98](#).

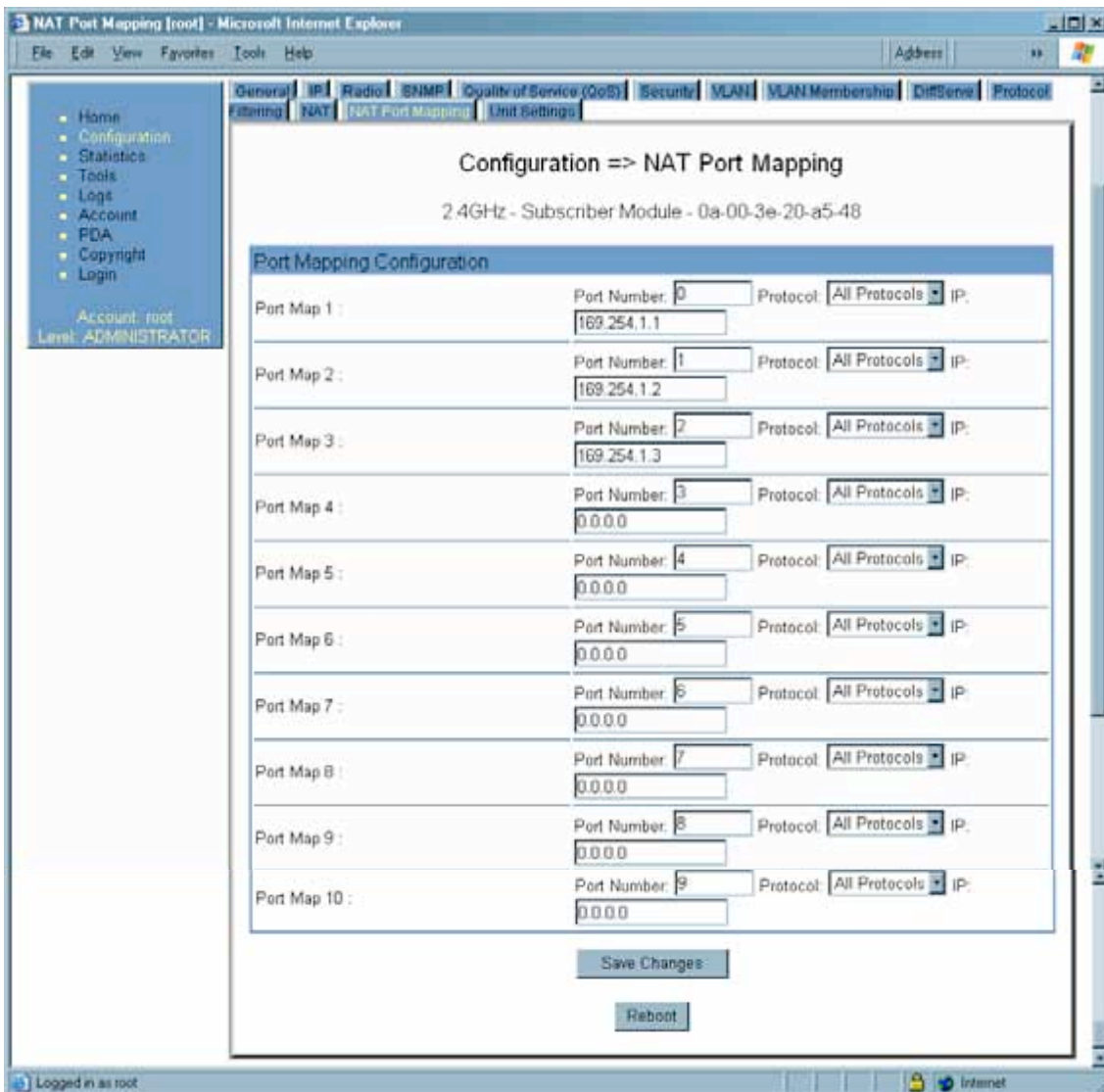


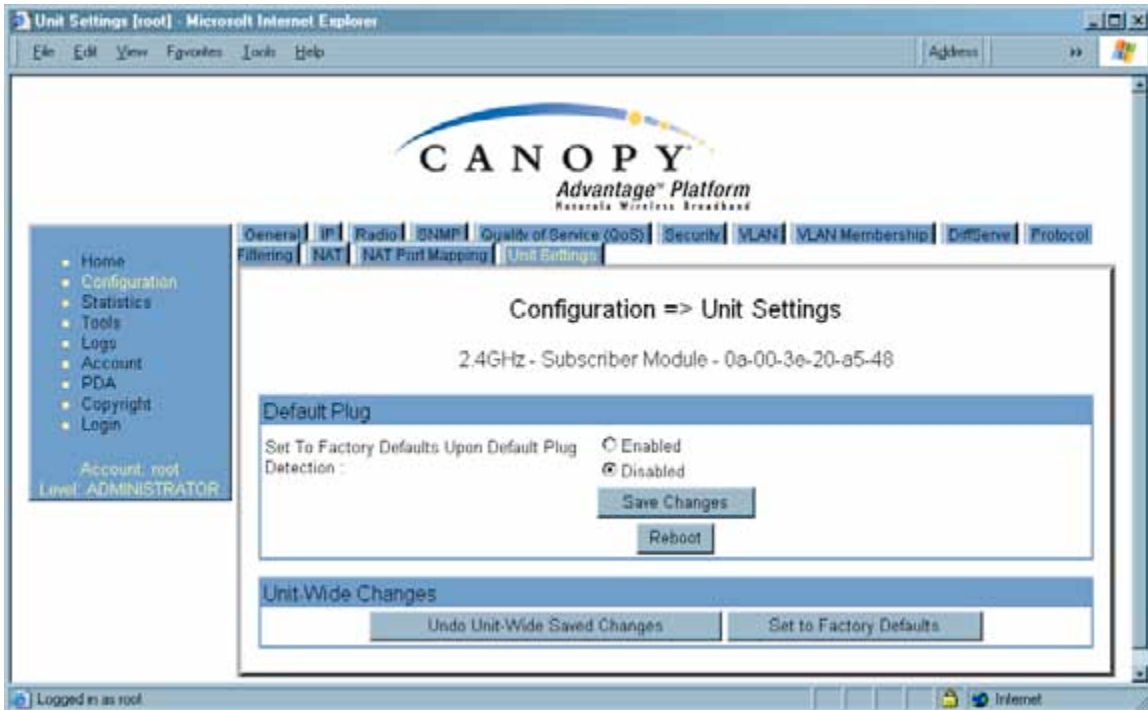
Figure 98: NAT Port Mapping tab of SM, example

In the NAT Port Mapping tab of the SM, you may set the following parameters.

### Port Map 1 to 10

## 18.2.13 Unit Settings Tab of the SM

An example of the Unit Settings tab in an SM is displayed in [Figure 99](#).



**Figure 99: Unit Settings tab of SM, example**

The Unit Settings tab of the SM contains an option for how the SM 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 373.

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.

#### **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.

#### **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.

### **18.3 SETTING THE CONFIGURATION SOURCE**

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

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

Most operators whose plans are typical should consult [Table 45](#).

**Table 45: Recommended combined settings for typical operations**

Most operators who use...	should set this parameter...	in this web page...	of this module...	to...
none	<b>Authentication Mode</b>	Configuration> Security	AP	<b>Authentication Disabled</b>
	<b>Configuration Source</b>	Configuration> General	AP	<b>SM</b>
BAM Release 2.0 (Consider upgrading to Prizm)	<b>Authentication Mode</b>	Configuration	AP	<b>Authentication Required</b>
	<b>Configuration Source</b>	Configuration	AP	<b>BAM+SM</b>
BAM Release 2.1 (Consider upgrading to Prizm)	<b>Authentication Mode</b>	Configuration	AP	<b>Authentication Required</b>
	<b>Configuration Source</b>	Configuration	AP	<b>BAM</b>
Prizm Release 2.0 and 2.1 (being used for BAM functionality)	<b>Authentication Mode</b>	Configuration	AP	<b>Authentication Required</b>
	<b>Configuration Source</b>	Configuration	AP	<b>BAM</b>

Operators whose plans are atypical should consider the results that are described in [Table 46](#) and [Table 47](#). For any SM whose **Authentication Mode** parameter is set to **Authentication Required**, the listed settings are derived as shown in [Table 46](#).

**Table 46: Where feature values are obtained for an SM with authentication required**

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

**NOTES:**  
 HPC represents the **Hi Priority Channel** (enable or disable).  
 Where *BAM, then SM* is the indication, parameters for which BAM does not send values are obtained from the SM. This is the case where the BAM server is operating on a BAM release that did not support the feature. This is also the case where the feature enable/disable flag in BAM is set to disabled. The values are those previously set or, if none ever were, then the default values.  
 Where *BAM* is the indication, values in the SM are disregarded.  
 Where *SM* is the indication, values that BAM sends for the SM are disregarded.  
 The high-priority channel is unavailable to Series P7 and P8 SMs that run Canopy Release 8.

For any SM whose **Authentication Mode** parameter is *not* set to **Authentication Required**, the listed settings are derived as shown in [Table 47](#).

**Table 47: Where feature values are obtained for an SM with authentication disabled**

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

BAM Release 2.0 sends only MIR values. BAM Release 2.1 and Prizm Release 2.0 and 2.1 send VLAN and high-priority channel values as well.

For the case where the **Configuration Source** parameter in the AP is set to **BAM**, the SM stores a value for the **Dynamic Learning** VLAN parameter that differs from its factory default. When Prizm does not send VLAN values (because **VLAN Enable** is set to **No** in Prizm), the SM

- uses this stored **Disable** value for **Dynamic Learning**.
- shows the following in the VLAN Configuration web page:
  - *either* **Enable** or **Disable** as the value of the **Dynamic Learning** parameter.
  - **Allow Learning : No** under **Active Configuration**.

For the case where the **Configuration Source** parameter in the AP is set to **BAM+SM**, and Prizm does not send VLAN values, the SM

- uses the configured value in the SM for **Dynamic Learning**. If the SM is set to factory defaults, then this value is **Enable**.
- shows under **Active Configuration** the result of the configured value in the SM. For example, if the SM is set to factory defaults, then the VLAN Configuration page shows **Allow Learning : Yes**.

This selection (**BAM+SM**) *is not* recommended where Prizm manages the VLAN feature in SMs.

## 18.4 CONFIGURING A BH TIMING MASTER FOR THE DESTINATION



**NOTE:**

The PTP 400 and PTP 600 series bridges (previously known as 30/60 Mbps and 150/300 Mbps Backhuls) are described in their own dedicated user guides. See [Products Not Covered by This User Guide](#) on Page 34.

If an ADMINISTRATOR-level password has been set in the BHM, you must log into the module before you can configure its parameters. See [Managing Module Access by Passwords](#) on Page 371.

### 18.4.1 General Tab of the BHM

An example of the General tab in a BHM is displayed in [Figure 100](#).

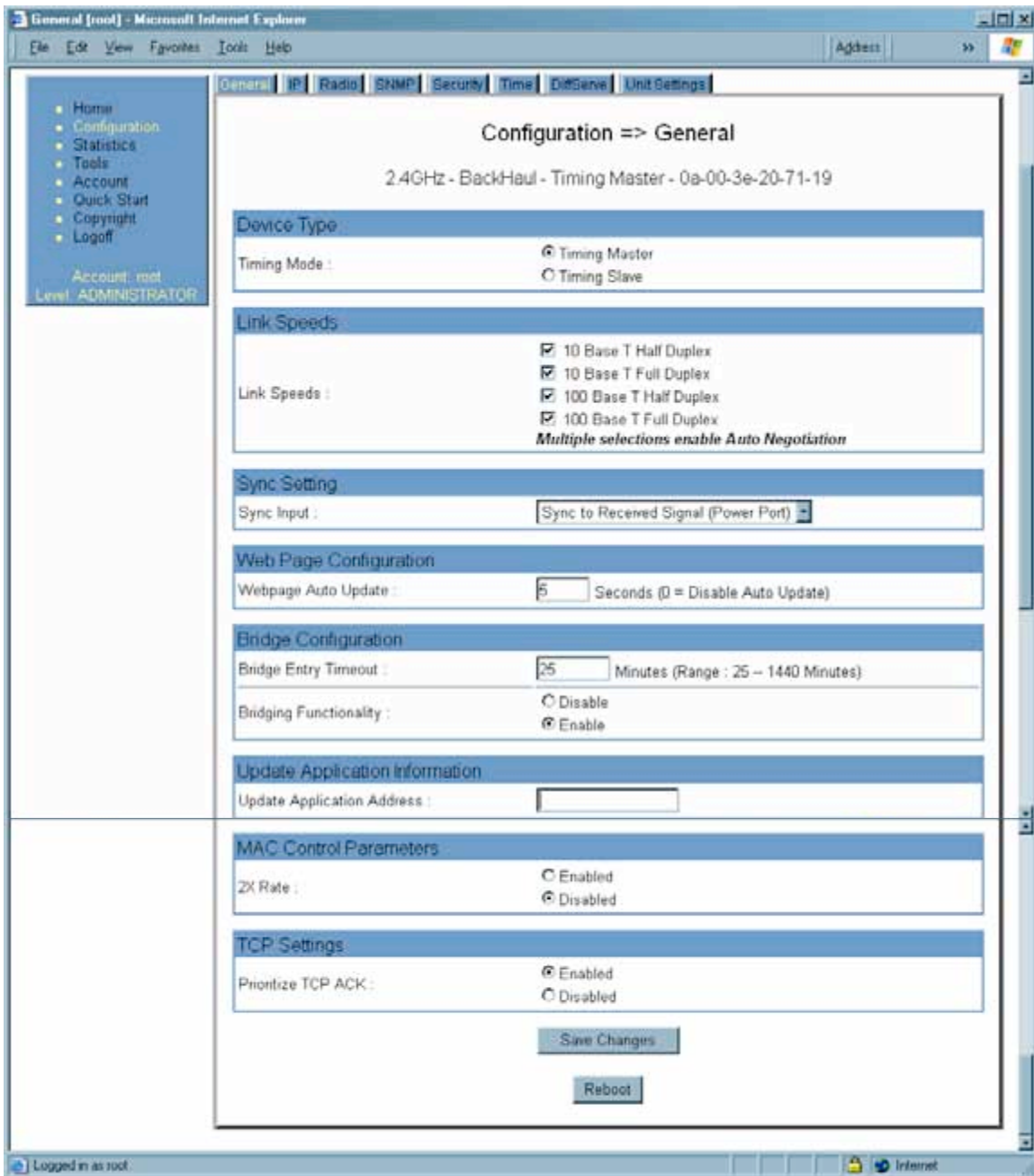


Figure 100: General tab of BHM, example

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

### Timing Mode

Select **Timing Master**. This BH will provide sync for the link. Whenever you toggle this parameter to Timing Master from Timing Slave, 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 BHM is made available.

### 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.

### Sync Input

Specify the type of synchronization for this BH timing master to use.

- Select **Sync to Received Signal (Power Port)** to set this BHM to receive sync from a connected CMMmicro.
- Select **Sync to Received Signal (Timing Port)** to set this BHM to receive sync from a connected CMM2, an AP in the cluster, an SM, or a BH timing slave.
- Select **Generate Sync Signal** where the BHM does not receive sync, and no AP or other BHM is active within the link range.

### 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. The Bridge Entry Timeout should be a longer period than the ARP (Address Resolution Protocol) cache timeout of the router that feeds the network.



#### **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 BHM. 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.



**Update Application Address**

For capabilities in future software releases, you can enter the address of the server to access for software updates on this BHM.

**2X Rate**

See [2X Operation](#) on Page 89.

**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. See [AP-SM Links](#) on Page 99.

The General tab of the BHM 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.

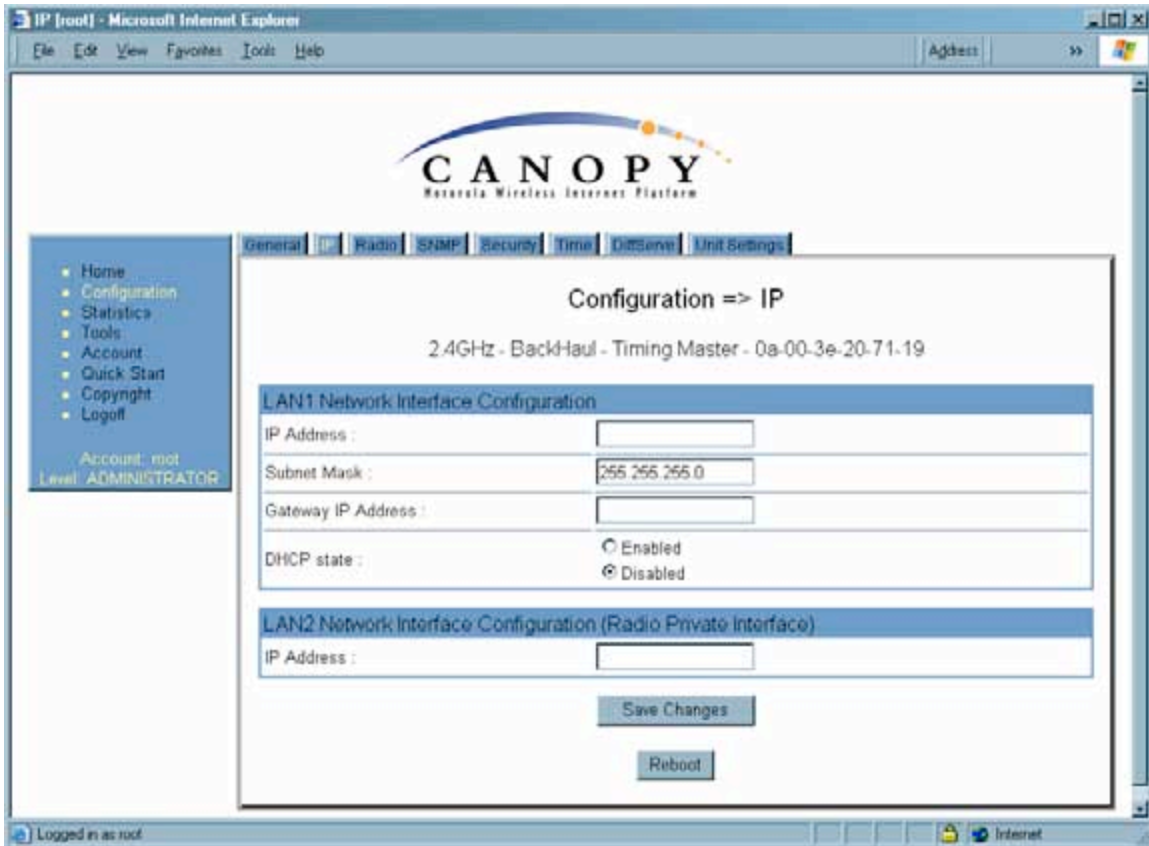
**Reboot**

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.

### 18.4.2 IP Tab of the BHM

An example of an IP tab in a BHM is displayed in [Figure 101](#).



**Figure 101: IP tab of BHM, example**

You may set the following IP Configuration page parameters.

#### **LAN1 Network Interface Configuration, IP Address**

Enter the *non-routable* IP address to be associated with the Ethernet connection on this module. (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 375.



#### **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 BHM 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 BHM 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.

**LAN2 Network Interface Configuration (RF Private Interface), IP Address**

Enter the IP address to be associated with this BHM for over-the-air access.

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.

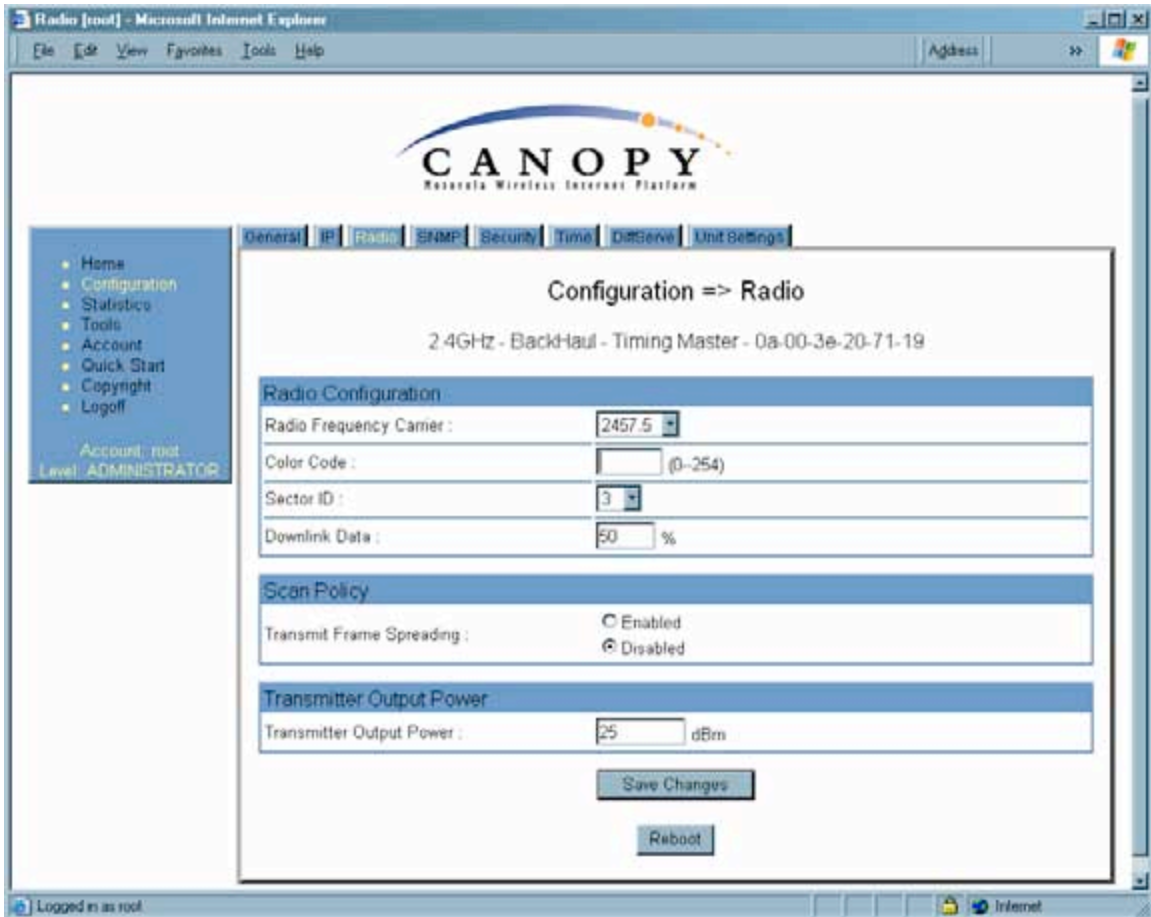
**Reboot**

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.

### 18.4.3 Radio Tab of the BHM

An example of the Radio tab in a BHM is displayed in [Figure 102](#).



**Figure 102: Radio tab of BHM, example**

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

#### Radio Frequency Carrier

Specify the frequency for the BHM to transmit. The default for this parameter is **None**. (The selection labeled **Factory** requires a special software key file for implementation.) In a 5.7-GHz BHM, this parameter displays both ISM and U-NII frequencies. In a 5.2-GHz BHM, this parameter displays only ISM frequencies. For a list of channels in the band, see [Considering Frequency Band Alternatives](#) on Page 136.

#### 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).