Perform the following procedure to set up the CMMmicro.

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

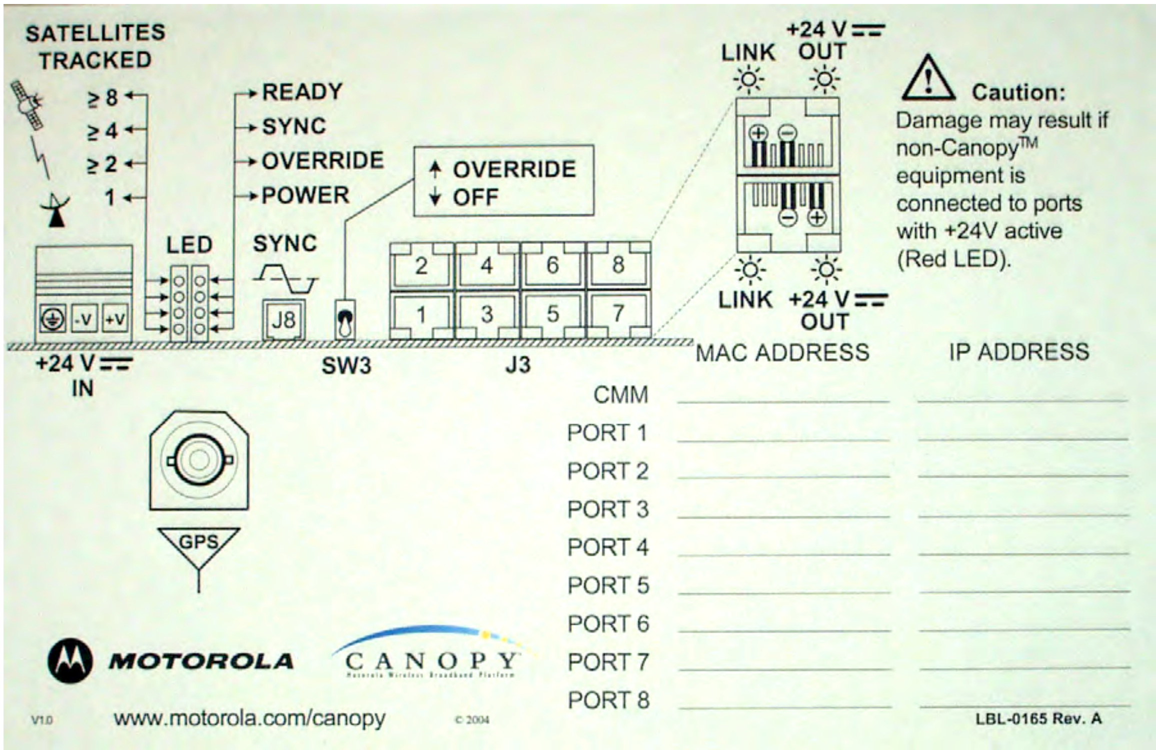
Procedure 17: Setting up a CMMmicro

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 74 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 75 on Page 220.) 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 76 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.

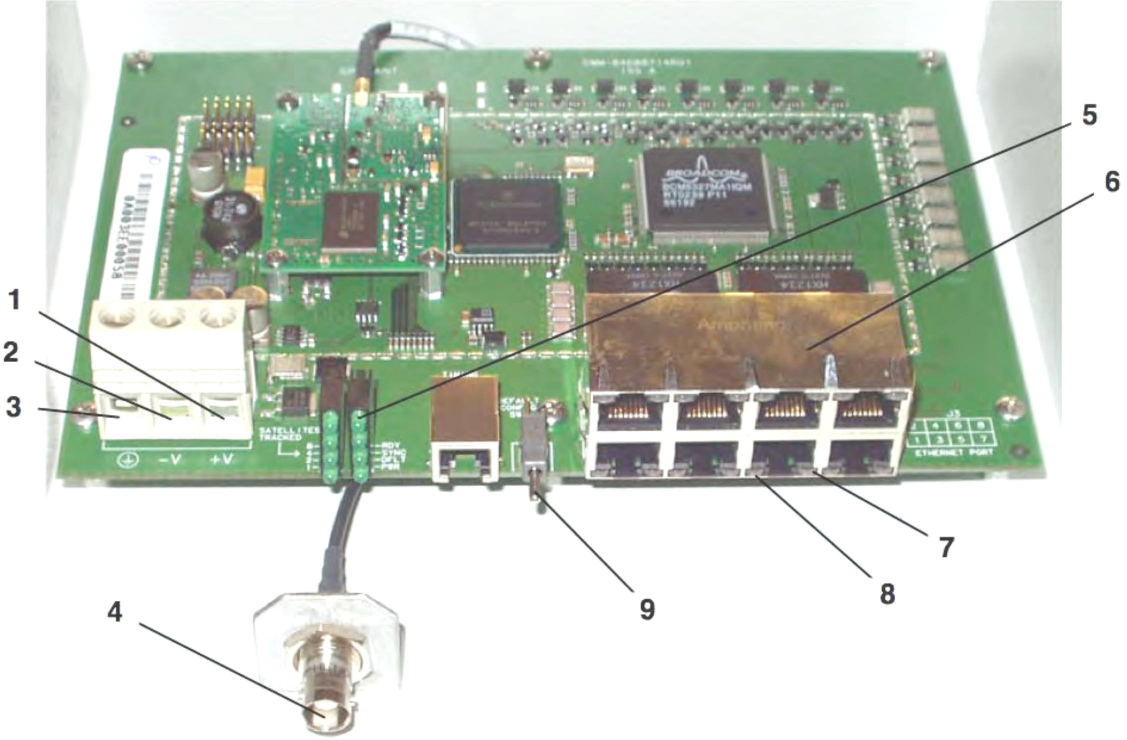
============================ **end of procedure** ============================



Caution: Damage may result if non-Canopy™ equipment is connected to ports with +24V active (Red LED).

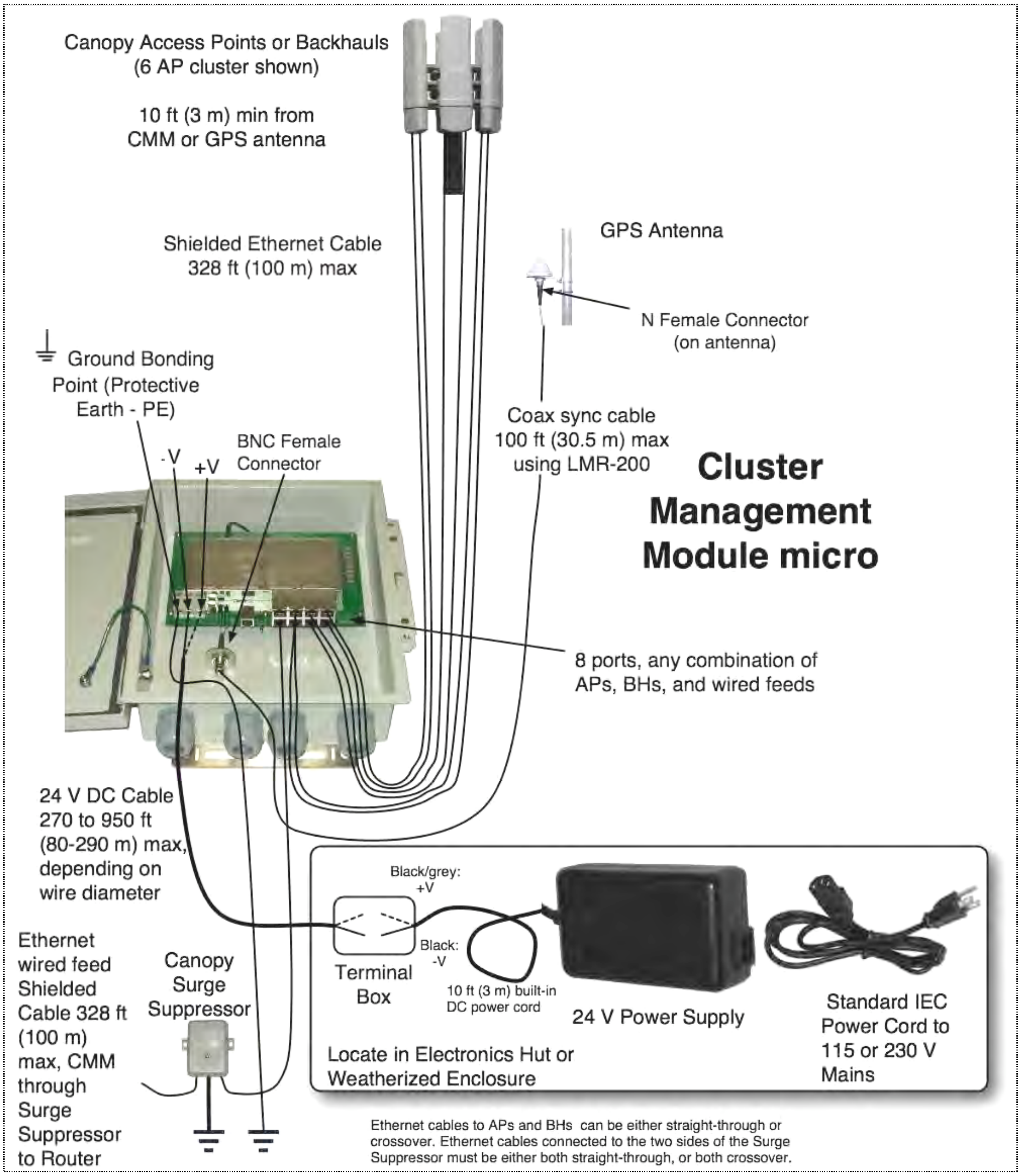
	MAC ADDRESS	IP ADDRESS
CMM		
PORT 1		
PORT 2		
PORT 3		
PORT 4		
PORT 5		
PORT 6		
PORT 7		
PORT 8		

Figure 74: 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, ≥ 4, and ≥ 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 75: CMMmicro circuit board

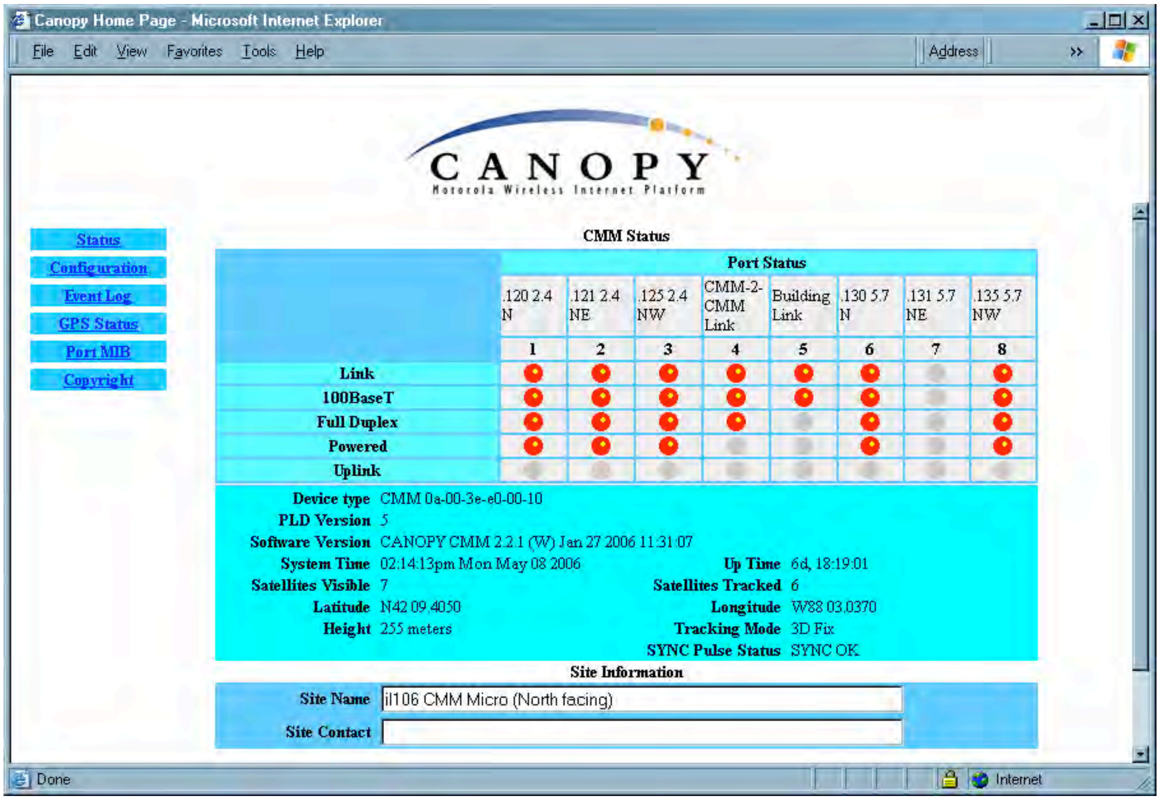


Ethernet cables to APs and BHs can be either straight-through or crossover. Ethernet cables connected to the two sides of the Surge Suppressor must be either both straight-through, or both crossover.

Figure 76: CMMmicro connections

16.4.8 Status Page of the CMMmicro

An example of a CMMmicro Status page is displayed in Figure 77.



CMM Status

	Port Status							
	.120 2.4 N	.121 2.4 NE	.125 2.4 NW	CMM-2-CMM Link	Building Link	.130 5.7 N	.131 5.7 NE	.135 5.7 NW
	1	2	3	4	5	6	7	8
Link	●	●	●	●	●	●	○	●
100BaseT	●	●	●	●	●	●	○	●
Full Duplex	●	●	●	●	○	●	○	●
Powered	●	●	●	○	○	●	○	●
Uplink	○	○	○	○	○	○	○	○

Device type	CMM 0a-00-3e-e0-00-10		
PLD Version	5		
Software Version	CANOPY CMM 2.2.1 (W) Jan 27 2006 11:31:07		
System Time	02:14:13pm Mon May 08 2006	Up Time	6d, 18:19:01
Satellites Visible	7	Satellites Tracked	6
Latitude	N42 09.4050	Longitude	W88 03.0370
Height	255 meters	Tracking Mode	3D Fix
		SYNC Pulse Status	SYNC OK

Site Information

Site Name: il106 CMM Micro (North facing)

Site Contact:

Figure 77: 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 75 on Page 220.) 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

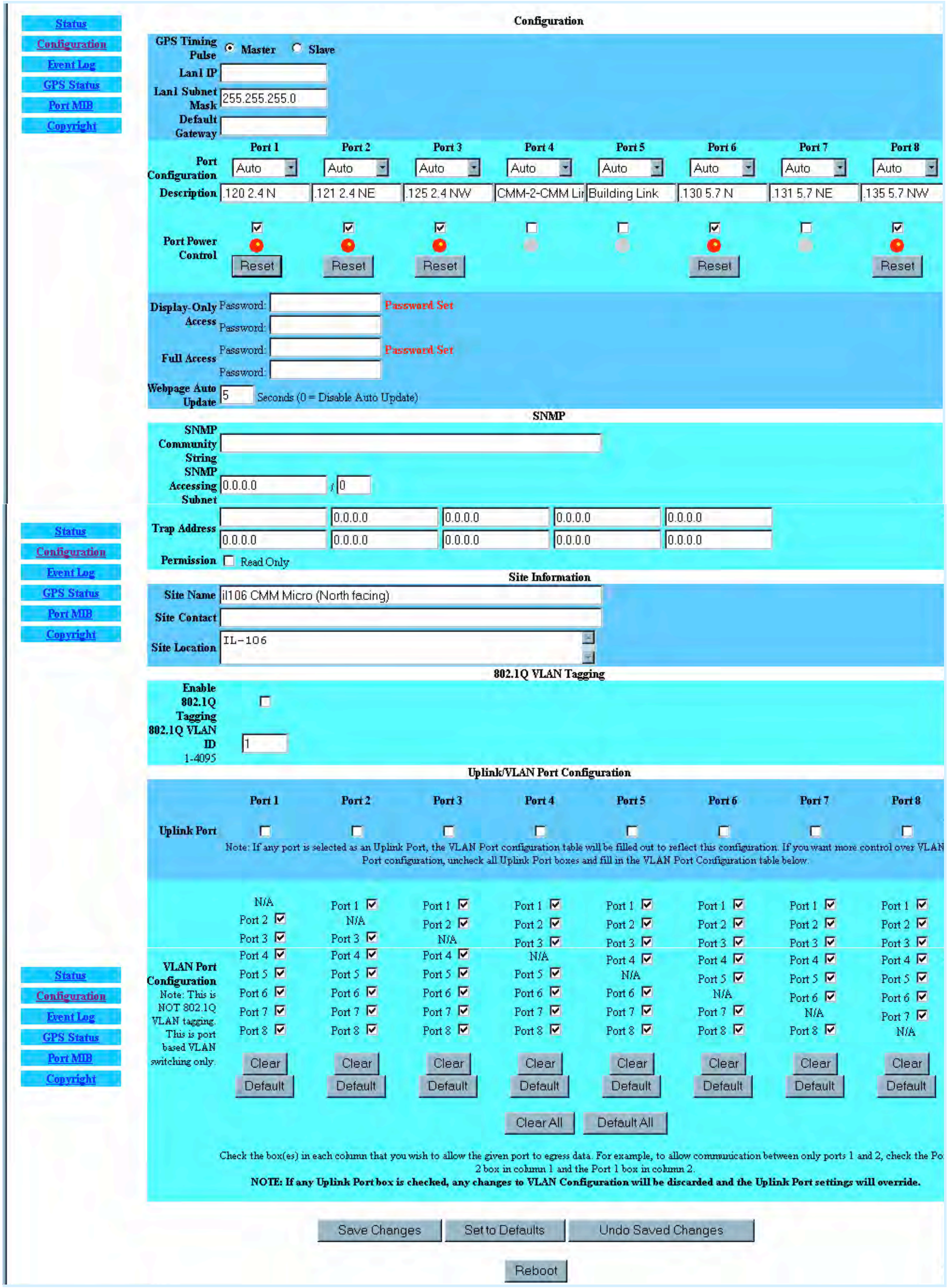
This field displays administrative information that has been entered on the Configuration page of the CMMmicro.

Site Contact

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

16.4.9 Configuration Page of the CMMmicro

An example of the CMMmicro Configuration page is displayed in Figure 78.



Configuration

GPS Timing Pulse: ● Master ○ Slave

Lan1 IP:

Lan1 Subnet Mask: 255.255.255.0

Default Gateway:

	Port 1	Port 2	Port 3	Port 4	Port 5	Port 6	Port 7	Port 8
Port Configuration	Auto	Auto	Auto	Auto	Auto	Auto	Auto	Auto
Description	120 2.4 N	121 2.4 NE	125 2.4 NW	CMM-2-CMM Lir	Building Link	130 5.7 N	131 5.7 NE	135 5.7 NW
Port Power Control	☑ ●	☑ ●	☑ ●	□	□	☑ ●	□	☑ ●

Display-Only Access Password: Password Set
Password:

Full Access Password: Password Set
Password:

Webpage Auto Update: 5 Seconds (0 = Disable Auto Update)

SNMP

SNMP Community String:

SNMP Accessing Subnet: 0.0.0.0 / 0

Trap Address:

	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0

Permission: □ Read Only

Site Information

Site Name: il106 CMM Micro (North facing)

Site Contact:

Site Location: IL-106

802.1Q VLAN Tagging

Enable 802.1Q Tagging: □

802.1Q VLAN ID 1-4095: 1

Uplink/VLAN Port Configuration

	Port 1	Port 2	Port 3	Port 4	Port 5	Port 6	Port 7	Port 8
Uplink Port	□	□	□	□	□	□	□	□

Note: If any port is selected as an Uplink Port, the VLAN Port configuration table will be filled out to reflect this configuration. If you want more control over VLAN Port configuration, uncheck all Uplink Port boxes and fill in the VLAN Port Configuration table below.

VLAN Port Configuration
Note: This is NOT 802.1Q VLAN tagging. This is port based VLAN switching only.

Port 1	Port 2	Port 3	Port 4	Port 5	Port 6	Port 7	Port 8
N/A	Port 1 ☑	Port 1 ☑	Port 1 ☑	Port 1 ☑	Port 1 ☑	Port 1 ☑	Port 1 ☑
Port 2 ☑	N/A	Port 2 ☑	Port 2 ☑	Port 2 ☑	Port 2 ☑	Port 2 ☑	Port 2 ☑
Port 3 ☑	Port 3 ☑	N/A	Port 3 ☑	Port 3 ☑	Port 3 ☑	Port 3 ☑	Port 3 ☑
Port 4 ☑	Port 4 ☑	Port 4 ☑	N/A	Port 4 ☑	Port 4 ☑	Port 4 ☑	Port 4 ☑
Port 5 ☑	Port 5 ☑	Port 5 ☑	Port 5 ☑	N/A	Port 5 ☑	Port 5 ☑	Port 5 ☑
Port 6 ☑	Port 6 ☑	Port 6 ☑	Port 6 ☑	Port 6 ☑	N/A	Port 6 ☑	Port 6 ☑
Port 7 ☑	Port 7 ☑	Port 7 ☑	Port 7 ☑	Port 7 ☑	Port 7 ☑	N/A	Port 7 ☑
Port 8 ☑	Port 8 ☑	Port 8 ☑	Port 8 ☑	Port 8 ☑	Port 8 ☑	Port 8 ☑	N/A

Check the box(es) in each column that you wish to allow the given port to egress data. For example, to allow communication between only ports 1 and 2, check the Po 2 box in column 1 and the Port 1 box in column 2.

NOTE: If any Uplink Port box is checked, any changes to VLAN Configuration will be discarded and the Uplink Port settings will override.

Figure 78: 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 377.

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

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 45.

Table 45: 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 75 on Page 220.) 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 377.

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 377.

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 78 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 78) 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 46.

Table 46: When changes become effective in CMMmicro

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

16.4.10 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

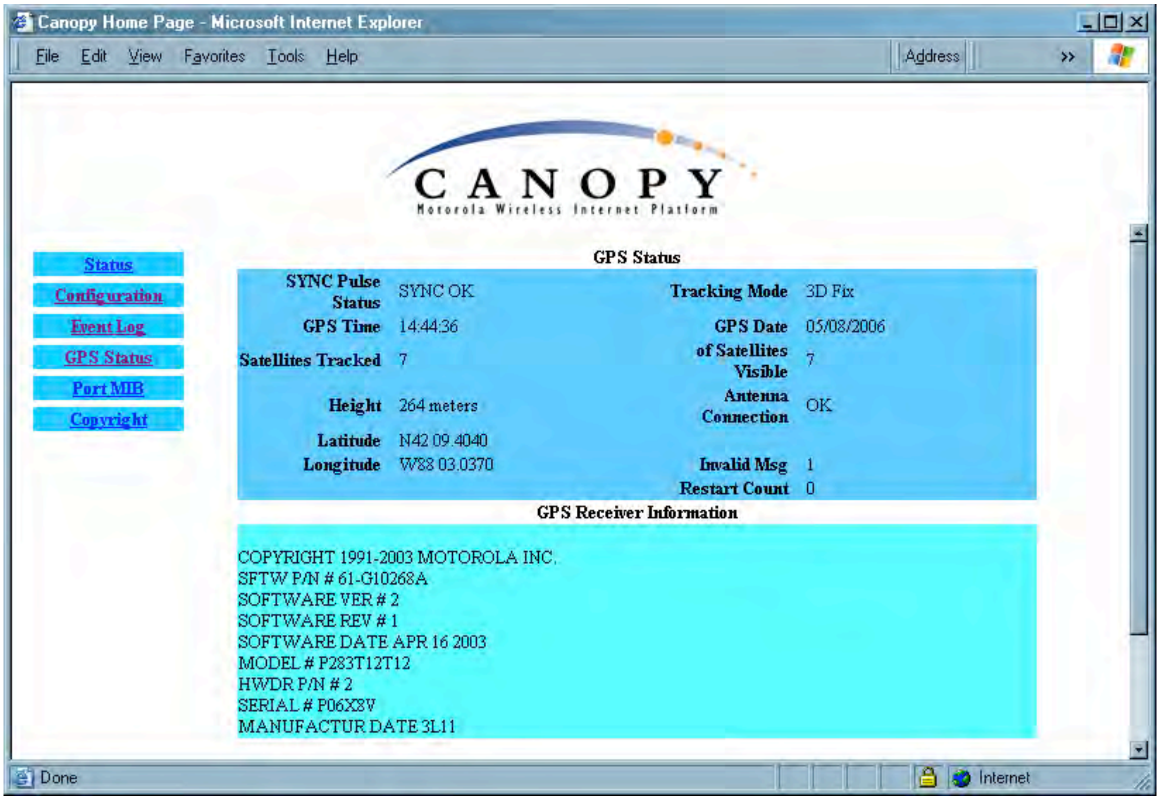
- Sync Input on Page 237.
- Sync Input on Page 296.

16.4.11 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.

16.4.12 GPS Status Page of the CMMmicro

An example of the CMMmicro GPS Status page is displayed in Figure 79.


Canopy Home Page - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address
CANOPY
Motorola Wireless Internet Platform
Status
Configuration
Event Log
GPS Status
Port MIB
Copyright
Done
Internet

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		
Longitude	W88 03.0370	Invalid Msg	1
		Restart Count	0

GPS Receiver Information

```
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 79: 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.

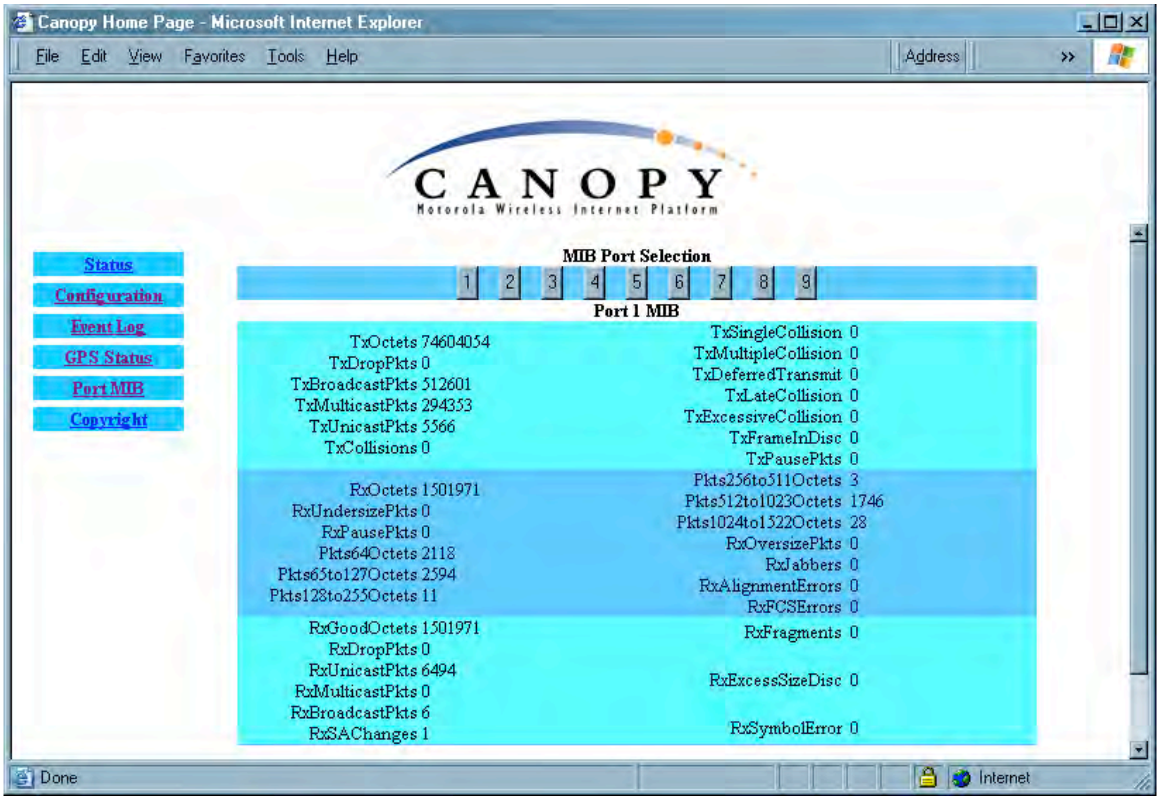
The other GPS Status fields are described under Satellites Visible on Page 222.

GPS Receiver Information

This field displays information about the GPS interface board.

16.4.13 Port MIB Page of the CMMmicro

An example of the Port MIB (Ethernet statistics) web page is displayed in Figure 80.


Canopy Home Page - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address
CANOPY
Motorola Wireless Internet Platform
Status
Configuration
Event Log
GPS Status
Port MIB
Copyright
MIB Port Selection
1 2 3 4 5 6 7 8 9
Done
Internet

Port 1 MIB

TxOctets	74604054	TxSingleCollision	0
TxDropPkts	0	TxMultipleCollision	0
TxBroadcastPkts	512601	TxDeferredTransmit	0
TxMulticastPkts	294353	TxLateCollision	0
TxUnicastPkts	5566	TxExcessiveCollision	0
TxCollisions	0	TxFrameInDisc	0
		TxPausePkts	0
RxOctets	1501971	Pkts256to511Octets	3
RxUndersizePkts	0	Pkts512to1023Octets	1746
RxPausePkts	0	Pkts1024to1522Octets	28
Pkts64Octets	2118	RxOversizePkts	0
Pkts65to127Octets	2594	RxJabbers	0
Pkts128to255Octets	11	RxAlignmentErrors	0
		RxFCSErrors	0
RxGoodOctets	1501971	RxFragments	0
RxDropPkts	0		
RxUnicastPkts	6494	RxExcessSizeDisc	0
RxMulticastPkts	0		
RxBroadcastPkts	6		
RxSAChanges	1	RxSymbolError	0

Figure 80: 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

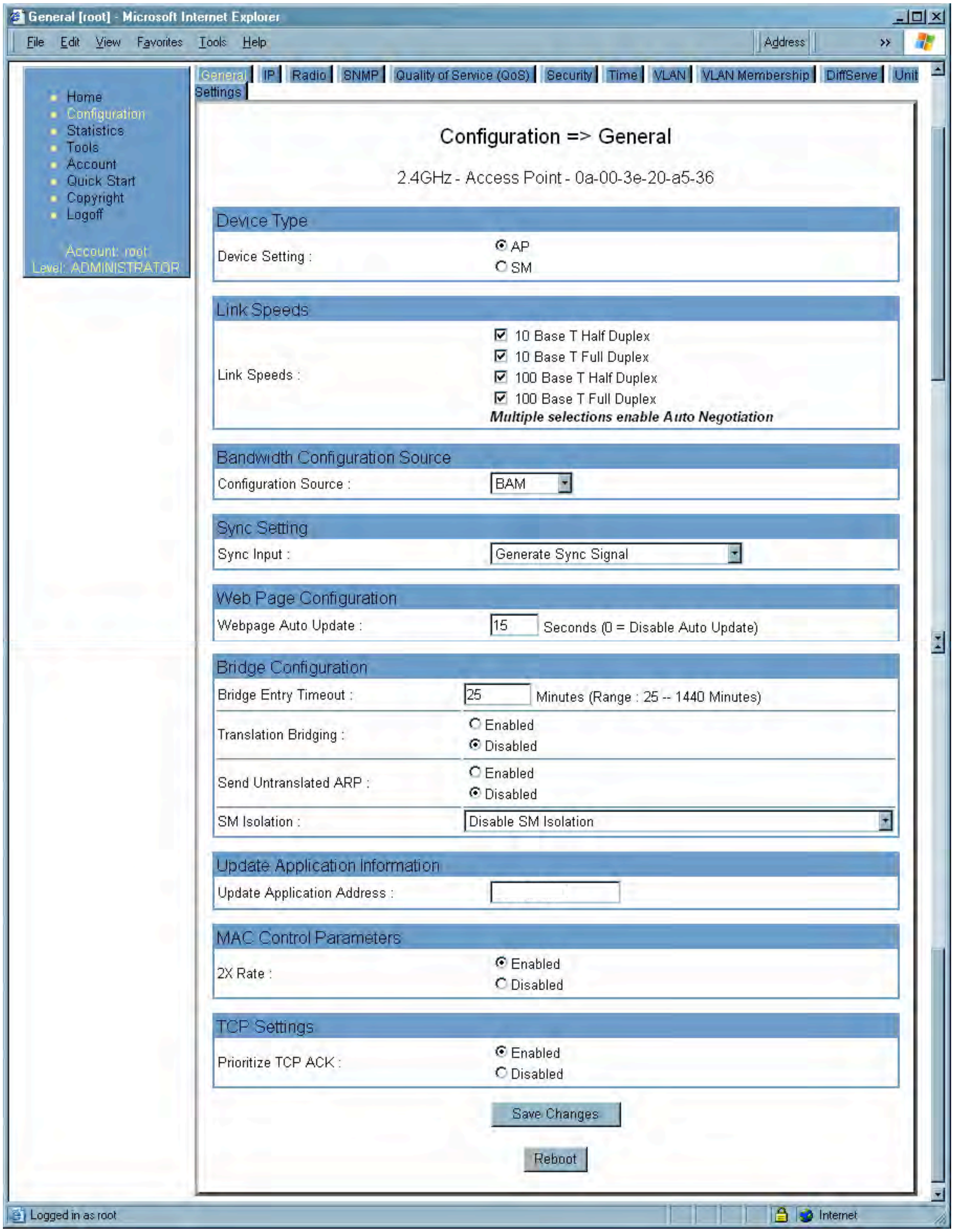
18 CONFIGURING FOR THE DESTINATION

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 373.

18.1.1 General Tab of the AP

An example of an AP General tab is displayed in Figure 81.


General [root] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address
Home
Configuration
Statistics
Tools
Account
Quick Start
Copyright
Logoff
Account: root
Level: ADMINISTRATOR
General | IP | Radio | SNMP | Quality of Service (QoS) | Security | Time | VLAN | VLAN Membership | DiffServe | Unit Settings
Logged in as root
Internet

Configuration => General

2.4GHz - Access Point - 0a-00-3e-20-a5-36

Device Type

Device Setting : ● AP ○ SM

Link Speeds

Link Speeds : ☑ 10 Base T Half Duplex ☑ 10 Base T Full Duplex ☑ 100 Base T Half Duplex ☑ 100 Base T Full Duplex

Multiple selections enable Auto Negotiation

Bandwidth Configuration Source

Configuration Source : BAM

Sync Setting

Sync Input : Generate Sync Signal

Web Page Configuration

Webpage Auto Update : 15 Seconds (0 = Disable Auto Update)

Bridge Configuration

Bridge Entry Timeout : 25 Minutes (Range : 25 -- 1440 Minutes)

Translation Bridging : ○ Enabled ● Disabled

Send Untranslated ARP : ○ Enabled ● Disabled

SM Isolation : Disable SM Isolation

Update Application Information

Update Application Address :

MAC Control Parameters

2X Rate : ● Enabled ○ Disabled

TCP Settings

Prioritize TCP ACK : ● Enabled ○ Disabled

Save Changes

Reboot

Figure 81: 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 81, 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 366. 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 83.

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 83 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 91.

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.

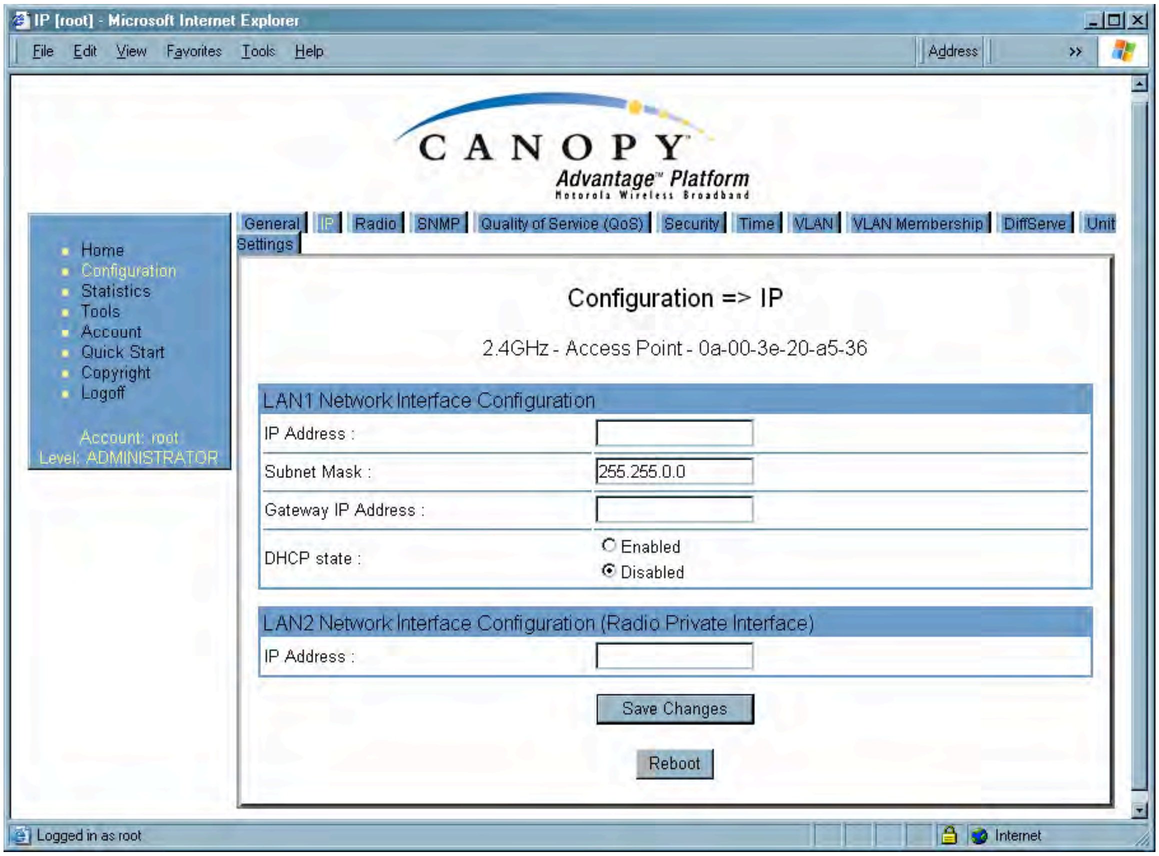
Reboot

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 82.



Configuration => IP

2.4GHz - Access Point - 0a-00-3e-20-a5-36

LAN1 Network Interface Configuration

IP Address :	
Subnet Mask :	255.255.0.0
Gateway IP Address :	
DHCP state :	○ Enabled ● Disabled

LAN2 Network Interface Configuration (Radio Private Interface)

IP Address :	

Figure 82: 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 377.

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

LAN1 Network Interface Configuration, Subnet Mask

Enter an appropriate subnet mask for the 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.

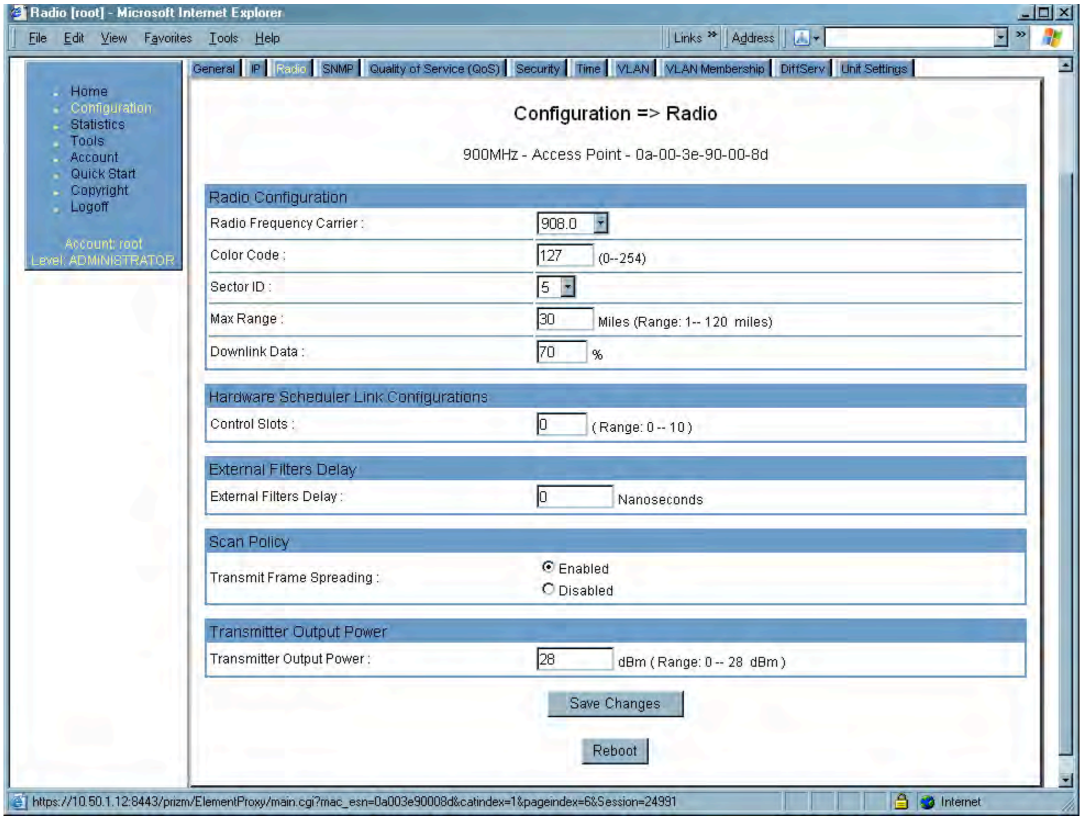
Reboot

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 83.


Radio [root] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Links Address
General IP Radio SNMP Quality of Service (QoS) Security Time VLAN VLAN Membership DiffServ Unit Settings
Home
Configuration
Statistics
Tools
Account
Quick Start
Copyright
Logoff
Account: root
Level: ADMINISTRATOR
Save Changes
Reboot
https://10.50.1.12:8443/prizm/ElementProxy/main.cgi?mac_esn=0a003e90008d&catindex=1&pageindex=6&Session=24991
Internet

Configuration => Radio

900MHz - Access Point - 0a-00-3e-90-00-8d

Radio Configuration

Radio Frequency Carrier :	908.0
Color Code :	127 (0--254)
Sector ID :	5
Max Range :	30 Miles (Range: 1-- 120 miles)
Downlink Data :	70 %

Hardware Scheduler Link Configurations

Control Slots :	0 (Range: 0 -- 10)

External Filters Delay

External Filters Delay :	0 Nanoseconds

Scan Policy

Transmit Frame Spreading :	● Enabled ○ Disabled

Transmitter Output Power

Transmitter Output Power :	28 dBm (Range: 0 -- 28 dBm)

Figure 83: 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 83, 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 27 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[7] 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 440.

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 47.

Table 47: 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.

[7] 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.

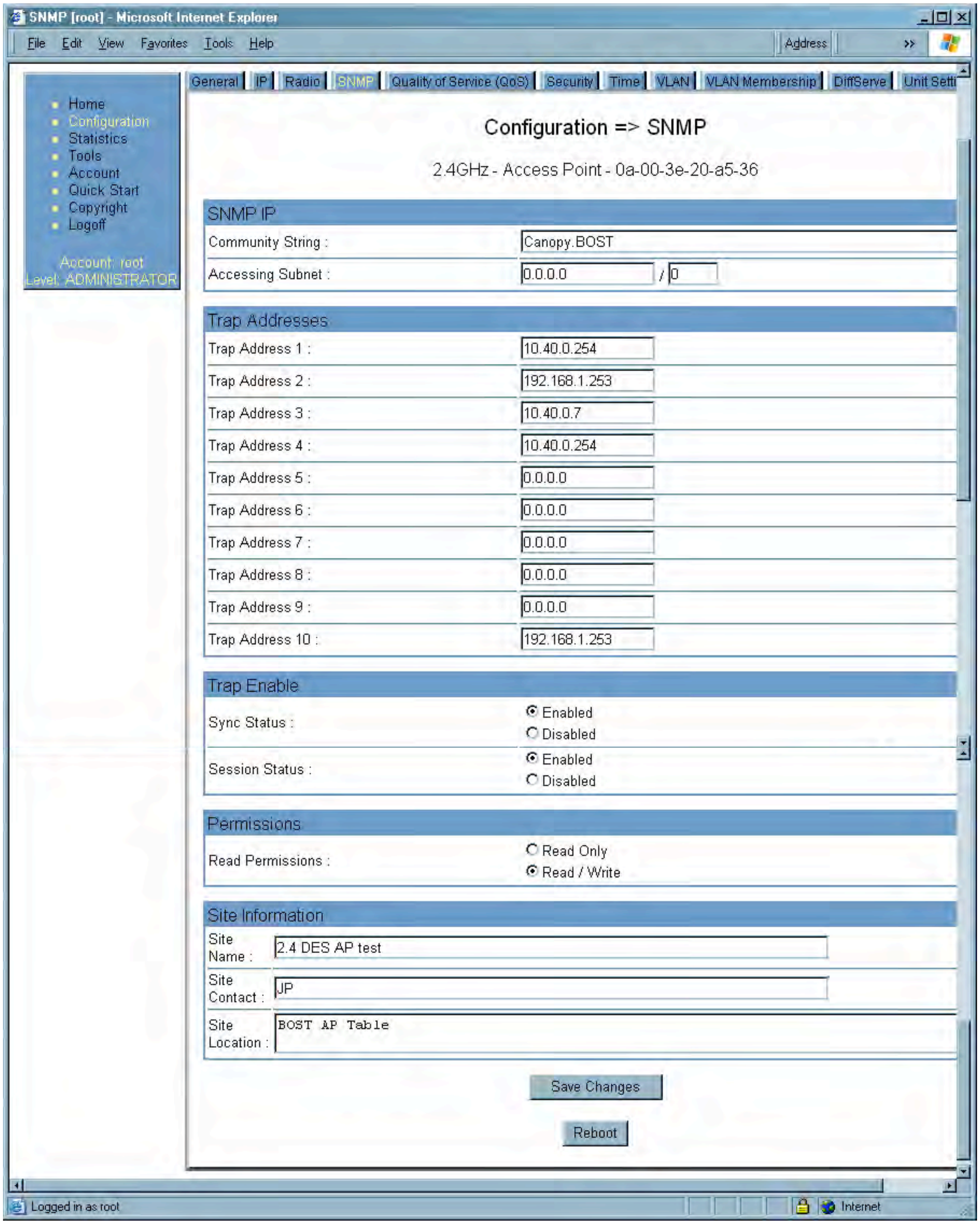
Reboot

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 84.


SNMP [root] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address
General IP Radio SNMP Quality of Service (QoS) Security Time VLAN VLAN Membership DiffServe Unit Setti
Home
Configuration
Statistics
Tools
Account
Quick Start
Copyright
Logoff
Account: root
Level: ADMINISTRATOR
Logged in as root
Internet

Configuration => SNMP

2.4GHz - Access Point - 0a-00-3e-20-a5-36

SNMP IP

Community String :	Canopy.BOST
Accessing Subnet :	0.0.0.0 / 0

Trap Addresses

Trap Address 1 :	10.40.0.254
Trap Address 2 :	192.168.1.253
Trap Address 3 :	10.40.0.7
Trap Address 4 :	10.40.0.254
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

Trap Enable

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

Permissions

Read Permissions :	○ Read Only ● Read / Write

Site Information

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

Save Changes

Reboot

Figure 84: 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 406. 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.

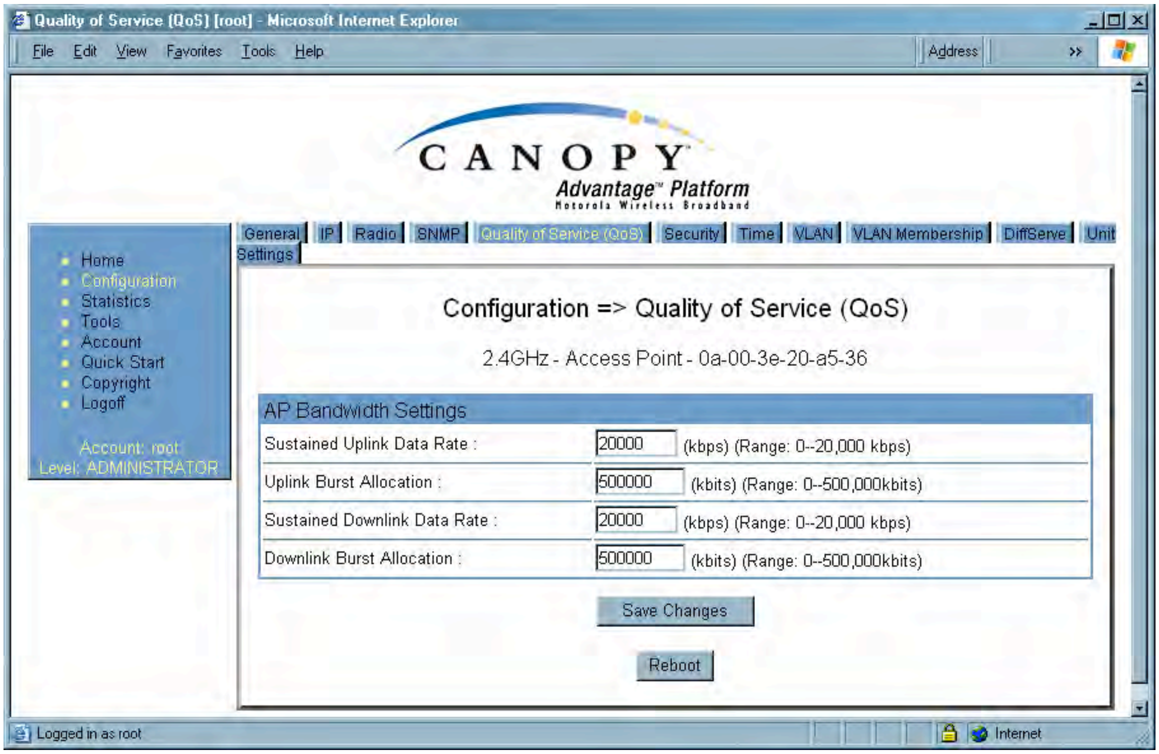
Reboot

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 85.



Configuration => Quality of Service (QoS)

2.4GHz - Access Point - 0a-00-3e-20-a5-36

AP Bandwidth Settings

Sustained Uplink Data Rate :	20000	(kbps) (Range: 0--20,000 kbps)
Uplink Burst Allocation :	500000	(kbits) (Range: 0--500,000kbits)
Sustained Downlink Data Rate :	20000	(kbps) (Range: 0--20,000 kbps)
Downlink Burst Allocation :	500000	(kbits) (Range: 0--500,000kbits)

Figure 85: 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 86
- Interaction of Burst Allocation and Sustained Data Rate Settings on Page 88
- 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 86
- Interaction of Burst Allocation and Sustained Data Rate Settings on Page 88
- 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 86
- Interaction of Burst Allocation and Sustained Data Rate Settings on Page 88
- 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 86
- Interaction of Burst Allocation and Sustained Data Rate Settings on Page 88
- 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.

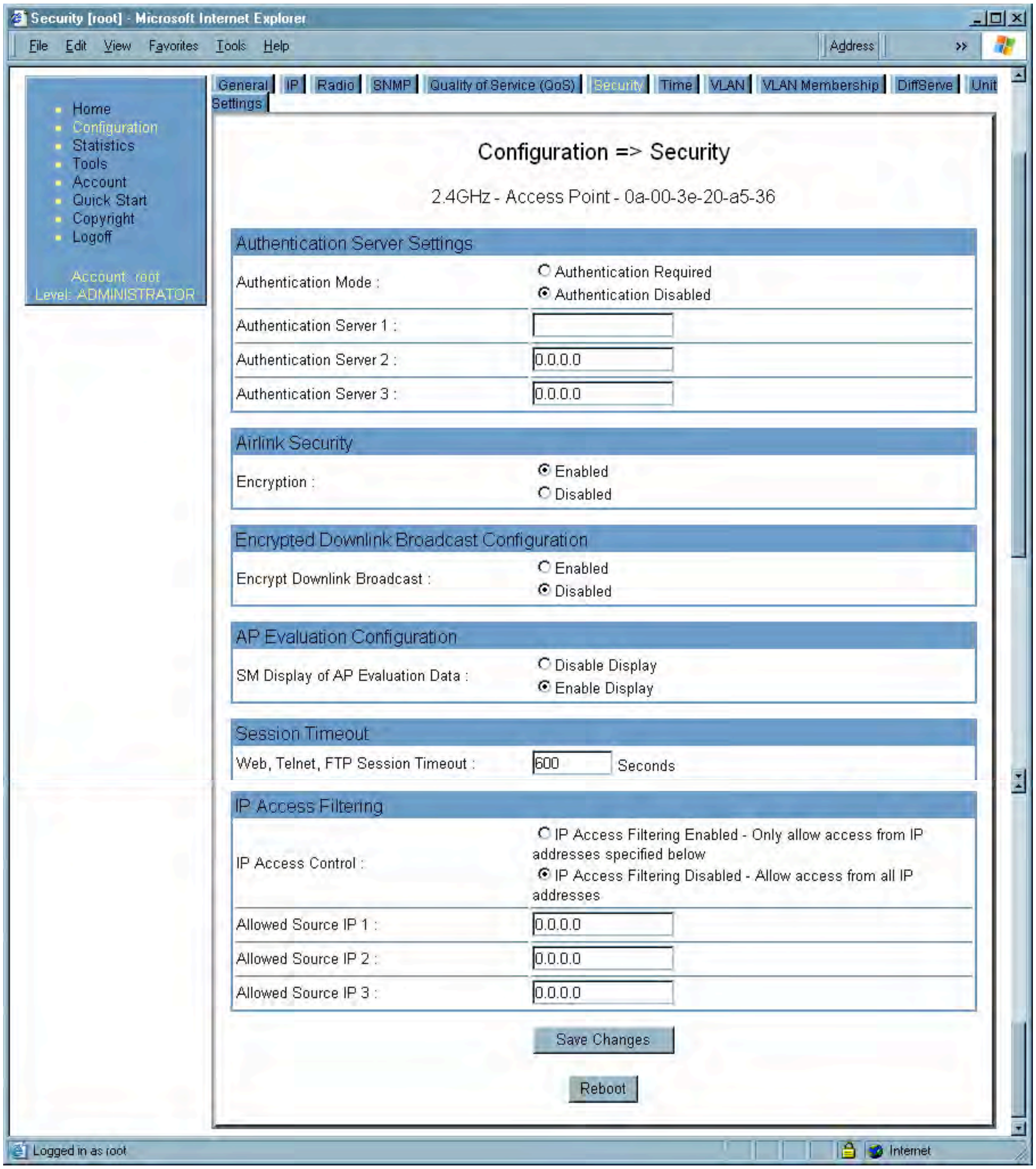
Reboot

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 86.



Configuration => Security

2.4GHz - Access Point - 0a-00-3e-20-a5-36

Authentication Server Settings

Authentication Mode :	○ Authentication Required ● Authentication Disabled
Authentication Server 1 :	
Authentication Server 2 :	0.0.0.0
Authentication Server 3 :	0.0.0.0

Airlink Security

Encryption :	● Enabled ○ Disabled

Encrypted Downlink Broadcast Configuration

Encrypt Downlink Broadcast :	○ Enabled ● Disabled

AP Evaluation Configuration

SM Display of AP Evaluation Data :	○ Disable Display ● Enable Display

Session Timeout

Web, Telnet, FTP Session Timeout :	600 Seconds

IP Access Filtering

IP Access Control :	○ IP Access Filtering Enabled - Only allow access from IP addresses specified below ● IP Access Filtering Disabled - Allow access from all IP addresses
Allowed Source IP 1 :	0.0.0.0
Allowed Source IP 2 :	0.0.0.0
Allowed Source IP 3 :	0.0.0.0

Figure 86: 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 380.

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.

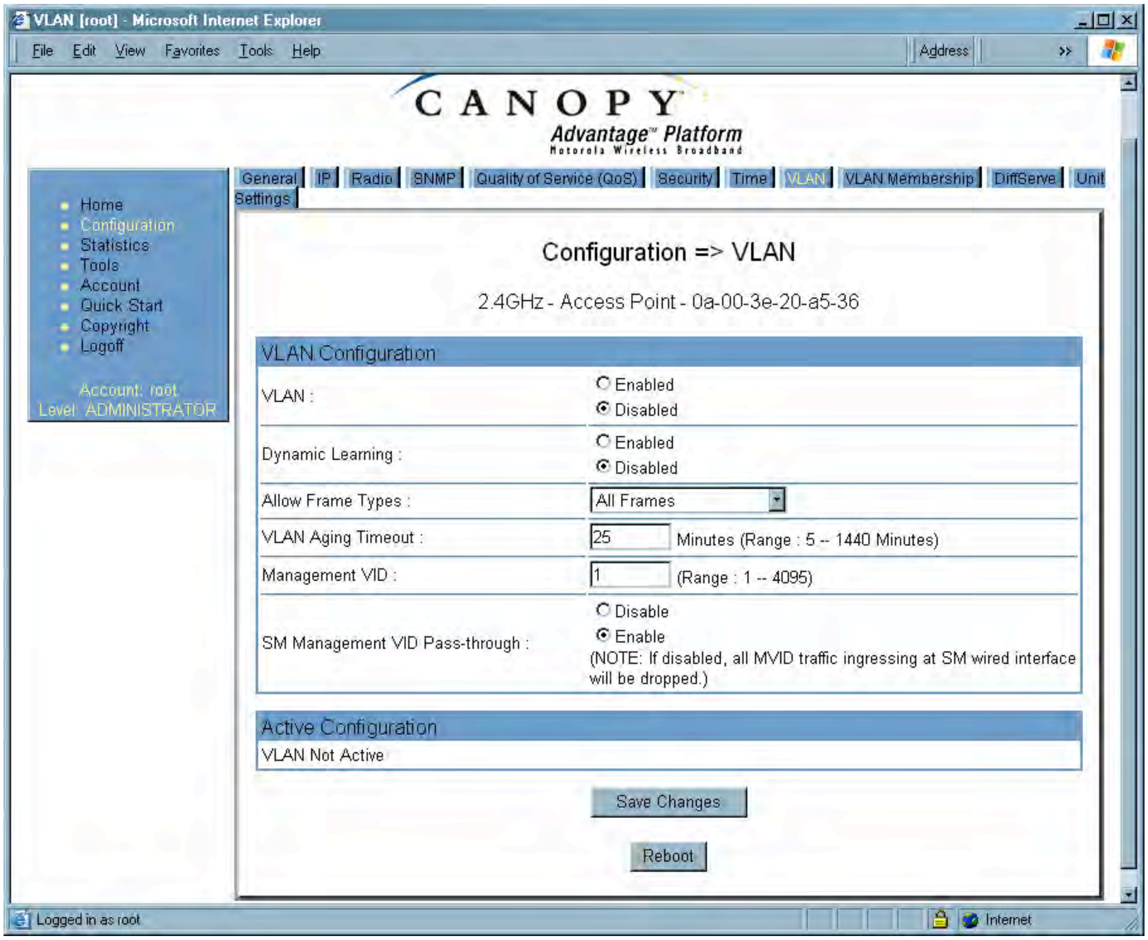
Reboot

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 87.


VLAN [root] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address
CANOPY
Advantage™ Platform
Motorola Wireless Broadband
General IP Radio SNMP Quality of Service (QoS) Security Time VLAN VLAN Membership DiffServe Unit Settings
Home
Configuration
Statistics
Tools
Account
Quick Start
Copyright
Logoff
Account: root
Level: ADMINISTRATOR
Save Changes
Reboot
Logged in as root
Internet

Configuration => VLAN

2.4GHz - Access Point - 0a-00-3e-20-a5-36

VLAN Configuration

VLAN :	○ Enabled ● Disabled
Dynamic Learning :	○ Enabled ● Disabled
Allow Frame Types :	All Frames
VLAN Aging Timeout :	25 Minutes (Range : 5 -- 1440 Minutes)
Management VID :	1 (Range : 1 -- 4095)
SM Management VID Pass-through :	○ Disable ● Enable (NOTE: If disabled, all MVID traffic ingressing at SM wired interface will be dropped.)

Active Configuration

VLAN Not Active

Figure 87: 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.

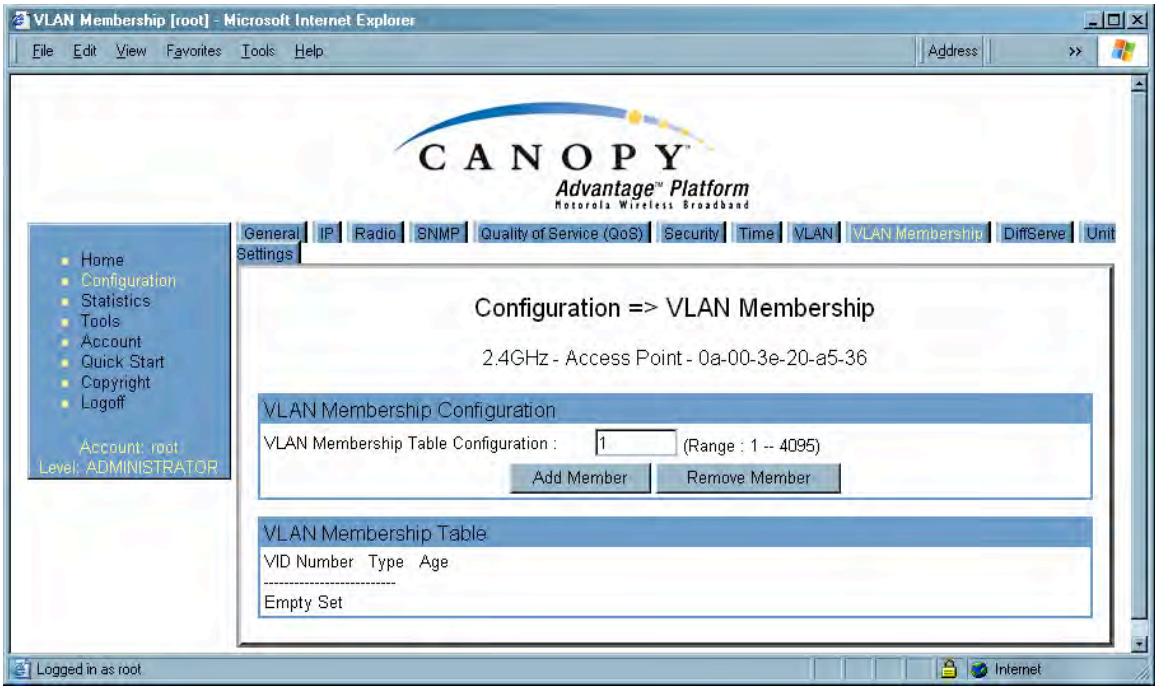
Reboot

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 88.



Configuration => VLAN Membership

2.4GHz - Access Point - 0a-00-3e-20-a5-36

VLAN Membership Configuration

VLAN Membership Table Configuration : 1 (Range : 1 -- 4095)

VLAN Membership Table

```
VID Number   Type   Age
-------------------------
Empty Set
```

Figure 88: VLAN Membership tab of AP, example

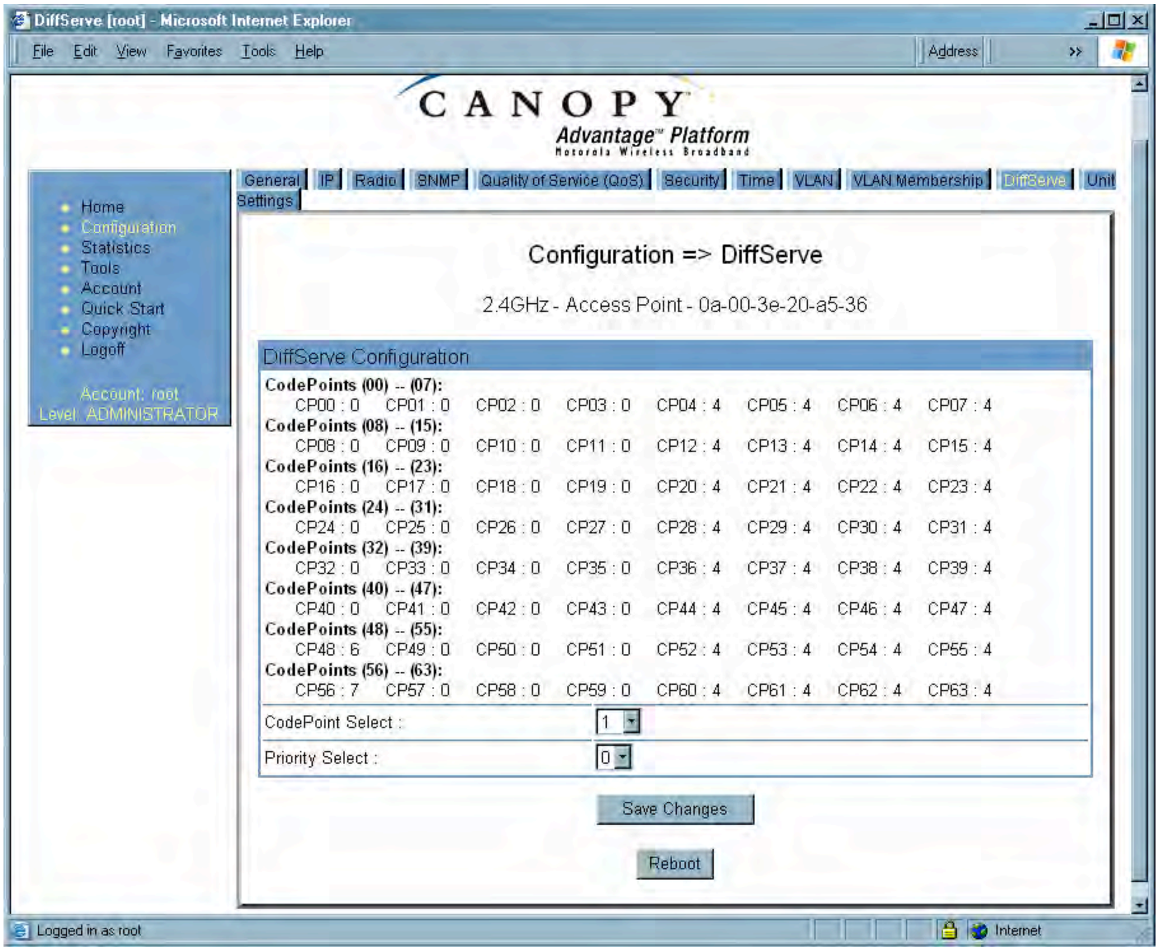
You may set the VLAN Membership tab parameter as follows.

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 89.



Configuration => DiffServe

2.4GHz - Access Point - 0a-00-3e-20-a5-36

DiffServe Configuration

```
CodePoints (00) -- (07):
    CP00 : 0   CP01 : 0   CP02 : 0   CP03 : 0   CP04 : 4   CP05 : 4   CP06 : 4   CP07 : 4
CodePoints (08) -- (15):
    CP08 : 0   CP09 : 0   CP10 : 0   CP11 : 0   CP12 : 4   CP13 : 4   CP14 : 4   CP15 : 4
CodePoints (16) -- (23):
    CP16 : 0   CP17 : 0   CP18 : 0   CP19 : 0   CP20 : 4   CP21 : 4   CP22 : 4   CP23 : 4
CodePoints (24) -- (31):
    CP24 : 0   CP25 : 0   CP26 : 0   CP27 : 0   CP28 : 4   CP29 : 4   CP30 : 4   CP31 : 4
CodePoints (32) -- (39):
    CP32 : 0   CP33 : 0   CP34 : 0   CP35 : 0   CP36 : 4   CP37 : 4   CP38 : 4   CP39 : 4
CodePoints (40) -- (47):
    CP40 : 0   CP41 : 0   CP42 : 0   CP43 : 0   CP44 : 4   CP45 : 4   CP46 : 4   CP47 : 4
CodePoints (48) -- (55):
    CP48 : 6   CP49 : 0   CP50 : 0   CP51 : 0   CP52 : 4   CP53 : 4   CP54 : 4   CP55 : 4
CodePoints (56) -- (63):
    CP56 : 7   CP57 : 0   CP58 : 0   CP59 : 0   CP60 : 4   CP61 : 4   CP62 : 4   CP63 : 4
```

CodePoint Select : 1

Priority Select : 0

Save Changes

Reboot

Figure 89: DiffServe tab of AP, example

You may set the following DiffServe tab parameters.

CodePoint 1 through CodePoint 47

CodePoint 49 through CodePoint 55

CodePoint 57 through CodePoint 63

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

Consistent with RFC 2474

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

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

The DiffServe tab also 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.

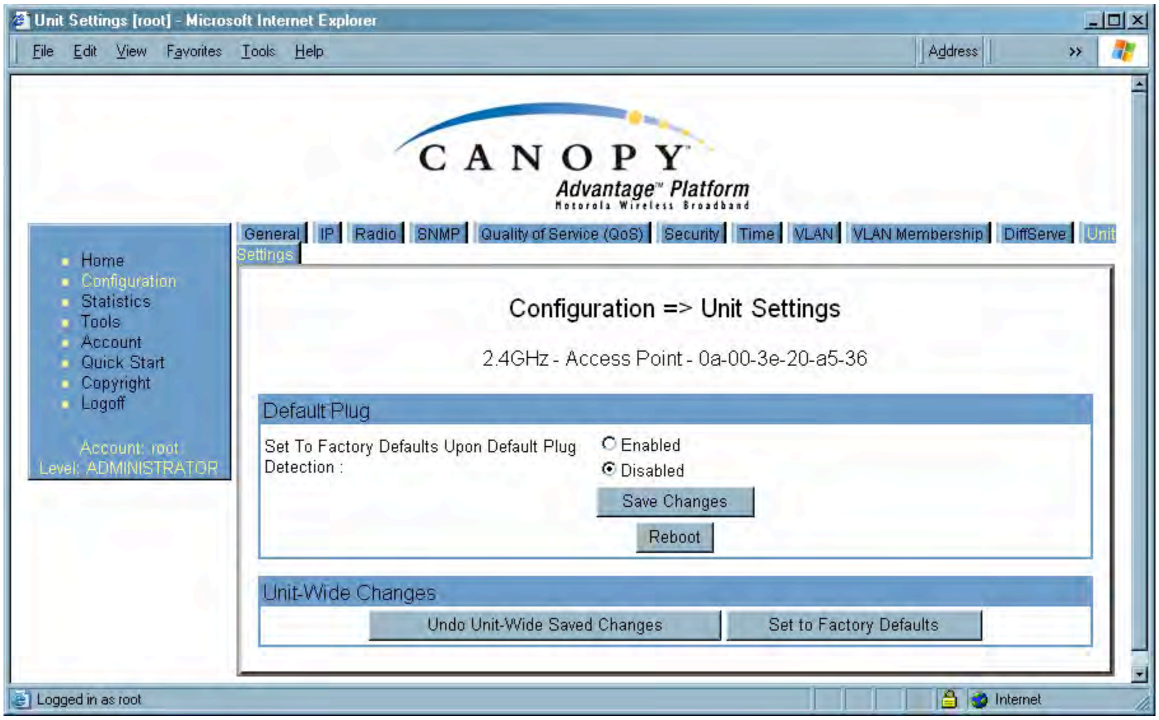
Reboot

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 90.



Configuration => Unit Settings

2.4GHz - Access Point - 0a-00-3e-20-a5-36

Default Plug

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

Unit-Wide Changes

Figure 90: 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 375.

The Unit Settings tab also contains the following buttons.

Save Changes

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

Reboot

When you click this button

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

Undo Unit-Wide Saved Changes

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

Set to Factory Defaults

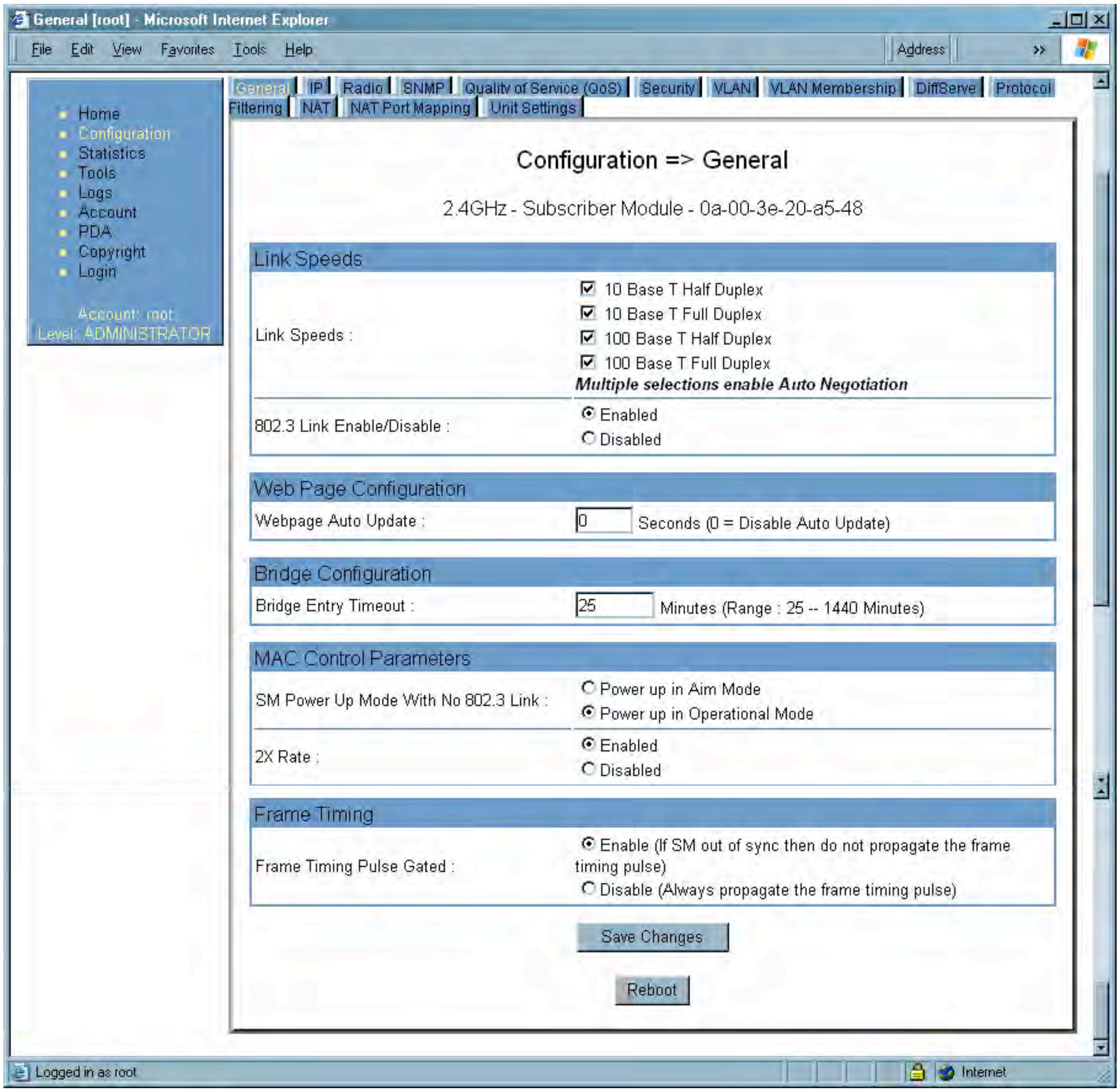
When you click this button, *all configurable parameters on all tabs* are reset to the factory settings.

18.2 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 373.

18.2.1 General Tab of the SM

An example of a General tab in the SM is displayed in Figure 91.


General [root] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address
Home
Configuration
Statistics
Tools
Logs
Account
PDA
Copyright
Login
Account: root
Level: ADMINISTRATOR
General IP Radio SNMP Quality of Service (QoS) Security VLAN VLAN Membership DiffServe Protocol Filtering NAT NAT Port Mapping Unit Settings
Save Changes
Reboot
Logged in as root
Internet

Configuration => General

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

Link Speeds

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

802.3 Link Enable/Disable :
● Enabled
○ Disabled

Web Page Configuration

Webpage Auto Update : 0 Seconds (0 = Disable Auto Update)

Bridge Configuration

Bridge Entry Timeout : 25 Minutes (Range : 25 -- 1440 Minutes)

MAC Control Parameters

SM Power Up Mode With No 802.3 Link :
○ Power up in Aim Mode
● Power up in Operational Mode

2X Rate :
● Enabled
○ Disabled

Frame Timing

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

Figure 91: 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 91.

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 369.

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.

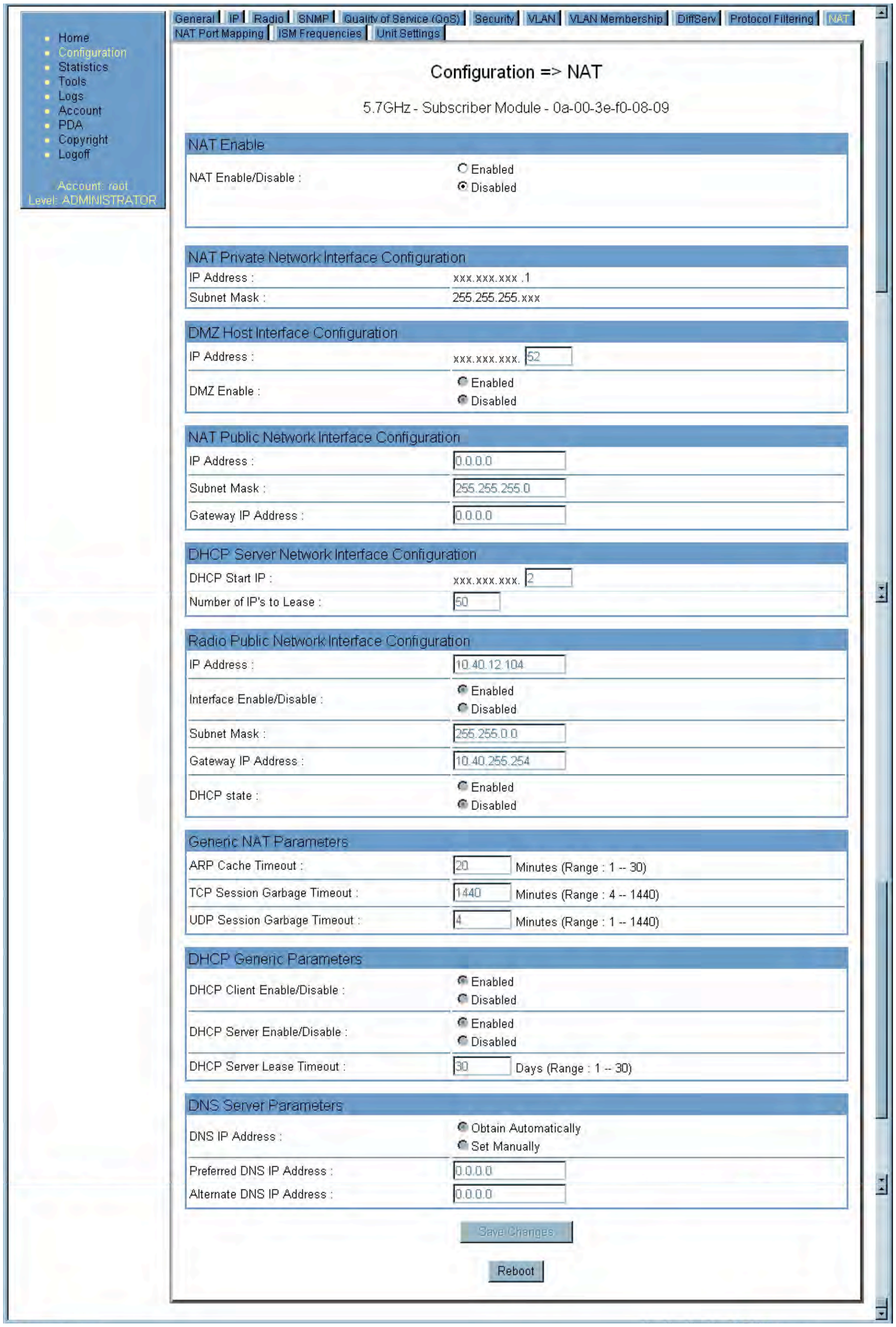
Reboot

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 92.



Configuration => NAT

5.7GHz - Subscriber Module - 0a-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. 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 :	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 :	20 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

Figure 92: NAT tab of SM with NAT disabled, example

This implementation is illustrated in Figure 46 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

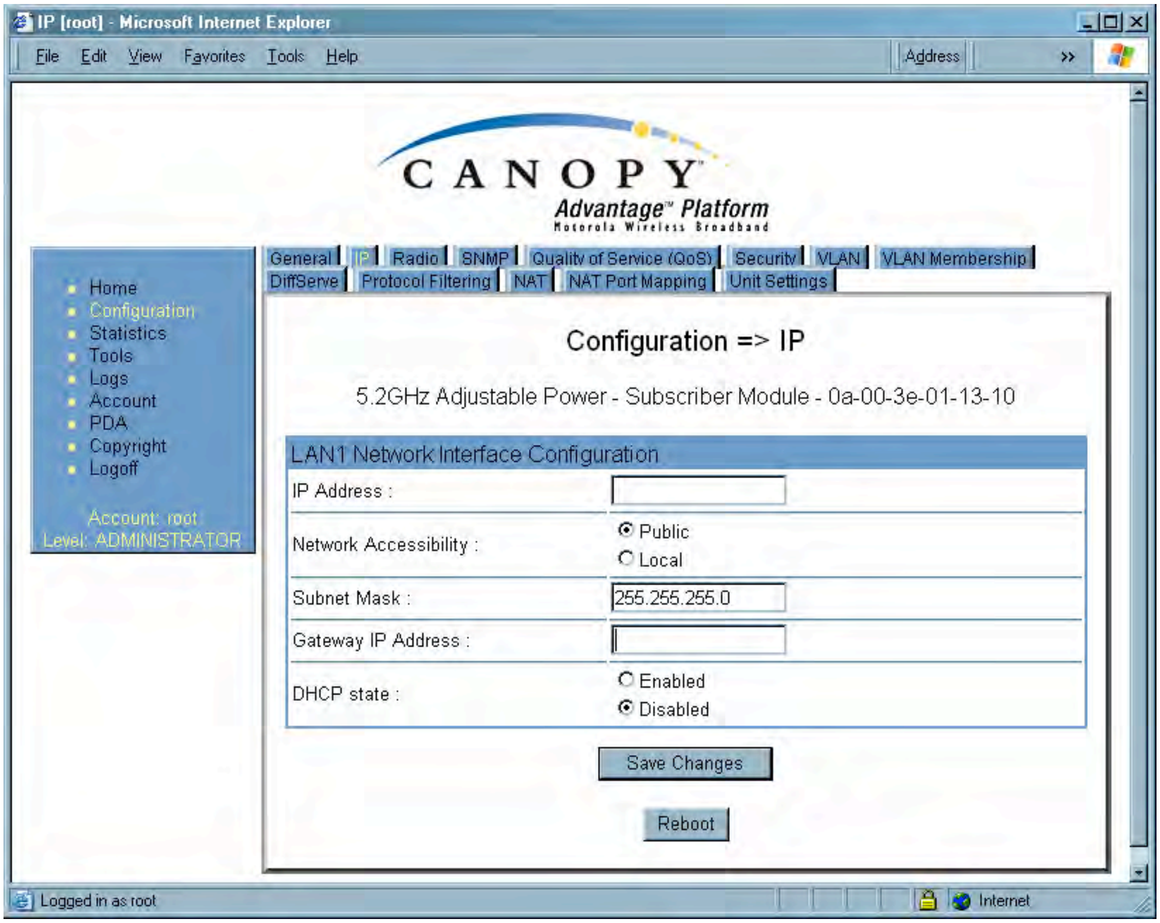
When you click this button, any changes that you made on all tabs are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

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 93.



Configuration => IP

5.2GHz Adjustable Power - Subscriber Module - 0a-00-3e-01-13-10

LAN1 Network Interface Configuration

IP Address :	
Network Accessibility :	● Public ○ Local
Subnet Mask :	255.255.255.0
Gateway IP Address :	
DHCP state :	○ Enabled ● Disabled

Figure 93: IP tab of SM with NAT disabled, example

This implementation is illustrated in Figure 46 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 377.

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