The sync is passed in a cable that connects Pins 1 and 6 of the RJ-11 timing ports of the two modules. When you connect modules in this way, you must also adjust configuration parameters to ensure that

- the AP is set to properly receive sync.
- the SM will not propagate sync to the AP if the SM itself ceases to receive sync.

Perform Procedure 35: Extending network sync on Page 374.

12.8.4 Physical Connections Involving the Remote AP

The SM to which you wire a remote AP can be either an SM that serves a customer or an SM that simply serves as a relay. Where the SM serves a customer, wire the remote AP to the SM as shown in Figure 38.

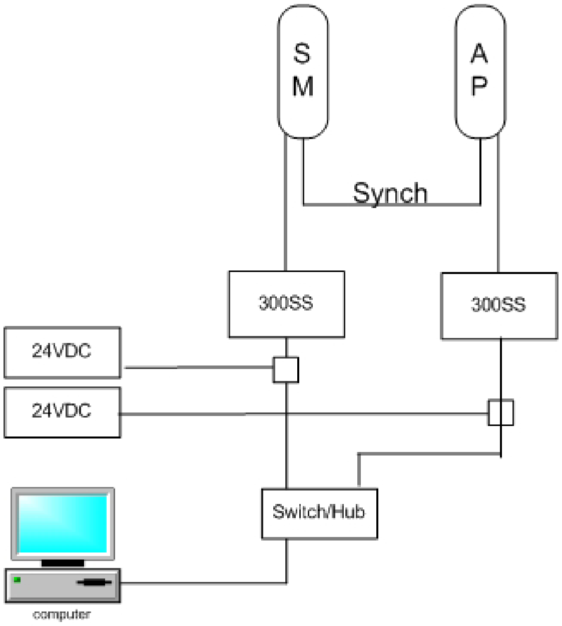


Figure 38: Remote AP wired to SM that also serves a customer

Where the SM simply serves as a relay, you must use a straight-through RJ-45 female-to-female coupler, and wire the SM to the remote AP as shown in Figure 39.

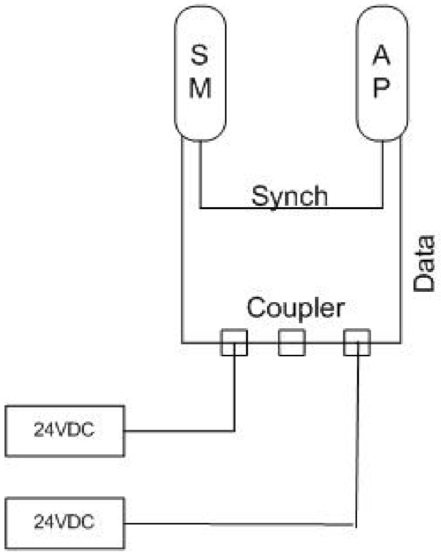


Figure 39: Remote AP wired to SM that serves as a relay

12.9 DIAGRAMMING NETWORK LAYOUTS

12.9.1 Accounting for Link Ranges and Data Handling Requirements

For aggregate throughput correlation to link distance in both point-to-multipoint and point-to-point links, see

- Link Performance and Encryption Comparisons on Page 61.
- all regulations that apply in your region and nation(s).

12.9.2 Avoiding Self Interference

For 5.2-, 5.4-, and 5.7-GHz modules, 20-MHz wide channels are centered every 5 MHz. For 2.4-GHz modules, 20-MHz wide channels are centered every 2.5 MHz. For 5.4-GHz OFDM modules, 10-MHz wide channels can be centered every 0.5 MHz. This allows you to customize the channel layout for interoperability where other Cyclone equipment is collocated, as well as select channels with the least background interference level.

CAUTION!
Regardless of whether 2.4-, 5.2-, 5.4-, or 5.7-GHz modules are deployed, channel separation between modules should be at least 20 MHz for 1X operation or 25 MHz for 2X.

Physical Proximity

A BH and an AP on the same tower require a CMM. The CMM properly synchronizes the *transmit start* times of all Cyclone modules to prevent interference and desensing of the modules. At closer distances without sync from a CMM, the frame structures cause self interference.

Furthermore, a BH and an AP on the same tower require that the effects of their differing *receive start* times be mitigated by either

- 100 vertical feet (30 meters) or more and as much spectral separation as possible within the same frequency band range.
- the use of the frame calculator to tune the Downlink Data % parameter in each, so that the receive start time in each is the same. See Using the Frame Calculator Tool (All) on Page 444.

Spectrum Analysis (Not available on Cyclone OFDM modules)

You can use an SM or BHS as a spectrum analyzer. See Mapping RF Neighbor Frequencies on Page 131. Through a toggle of the **Device Type** parameter, you can temporarily transform an AP into an SM to use it as a spectrum analyzer.

Power Reduction to Mitigate Interference

Where any module (SM, AP, BH timing master, or BH timing slave) is close enough to another module that self-interference is possible, you can set the SM to operate at less than full power. To do so, perform the following steps.

> ***CAUTION!***
> Too low a setting of the **Transmitter Output Power** parameter can cause a link to a distant module to drop. A link that drops for this reason requires Ethernet access to the GUI to re-establish the link.

Procedure 3: Reducing transmitter output power

1. Access the Radio tab of the module.
2. In the **Transmitter Output Power** parameter, reduce the setting.
3. Click **Save Changes**.
4. Click **Reboot**.
5. Access the Session Status tab in the Home web page of the SM.
6. Assess whether the link achieves good **Power Level** and **Jitter** values.
   NOTE: The received **Power Level** is shown in dBm and should be maximized. **Jitter** should be minimized. However, better/lower jitter should be favored over better/higher dBm. For historical reasons, **RSSI** is also shown and is the unitless measure of power. The best practice is to use **Power Level** and ignore **RSSI**, which implies more accuracy and precision than is inherent in its measurement.
7. Access the Link Capacity Test tab in the Tools web page of the module.
8. Assess whether the desired links for this module achieve
   - uplink efficiency greater than 90%.
   - downlink efficiency greater than 90%.
9. If the desired links fail to achieve any of the above measurement thresholds, then
   a. access the module by direct Ethernet connection.
   b. access the Radio tab in the Configuration web page of the module.
   c. in the **Transmitter Output Power** parameter, increase the setting.

d. click **Save Changes**.

e. click **Reboot**.

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

12.9.3 Avoiding Other Interference

Where signal strength cannot dominate noise levels, the network experiences

- bit error corrections.
- packet errors and retransmissions.
- lower throughput (because bandwidth is consumed by retransmissions) and high latency (due to resends).

Be especially cognitive of these symptoms for 900-MHz links. Where you see these symptoms, attempt the following remedies:

- Adjust the position of the SM.
- Deploy a band-pass filter at the AP.
- Consider adding a remote AP closer to the affected SMs. (See Deploying a Remote AP on Page 148.)

Certain other actions, which may seem to be potential remedies, *do not* resolve high noise level problems:

- *Do not* deploy an omnidirectional antenna.
- *Do not* set the antenna gain above the regulated level.
- *Do not* deploy a band-pass filter in the expectation that this can mitigate co-channel interference.

13 ENGINEERING YOUR IP COMMUNICATIONS

13.1 UNDERSTANDING ADDRESSES

A basic understanding of Internet Protocol (IP) address and subnet mask concepts is required for engineering your IP network.

13.1.1 IP Address

The IP address is a 32-bit binary number that has four parts (octets). This set of four octets has two segments, depending on the class of IP address. The first segment identifies the network. The second identifies the hosts or devices on the network. The subnet mask marks a boundary between these two sub-addresses.

13.2 DYNAMIC OR STATIC ADDRESSING

For any computer to communicate with a Cyclone module, the computer must be configured to either

- use DHCP (Dynamic Host Configuration Protocol). In this case, when not connected to the network, the computer derives an IP address on the 169.254 network within two minutes.
- have an assigned static IP address (for example, 169.254.1.5) on the 169.254 network.

IMPORTANT!
If an IP address that is set in the module is not the 169.254.x.x network address, then the network operator must assign the computer a static IP address in the same subnet.

13.2.1 When a DHCP Server is Not Found

To operate on a network, a computer requires an IP address, a subnet mask, and possibly a gateway address. Either a DHCP server automatically assigns this configuration information to a computer on a network or an operator must input these items.

When a computer is brought on line and a DHCP server is not accessible (such as when the server is down or the computer is not plugged into the network), Microsoft and Apple operating systems default to an IP address of 169.254.x.x and a subnet mask of 255.255.0.0 (169.254/16, where /16 indicates that the first 16 bits of the address range are identical among all members of the subnet).

13.3 NETWORK ADDRESS TRANSLATION (NAT)

13.3.1 NAT, DHCP Server, DHCP Client, and DMZ in SM

The Cyclone system provides NAT (network address translation) for SMs in the following combinations of NAT and DHCP (Dynamic Host Configuration Protocol):

- NAT Disabled (as in earlier releases)
- NAT with DHCP Client and DHCP Server
- NAT with DHCP Client
- NAT with DHCP Server
- NAT without DHCP

NAT

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.

In the Cyclone system, NAT supports many protocols, including HTTP, ICMP (Internet Control Message Protocols), and FTP (File Transfer Protocol). For virtual private network (VPN) implementation, L2TP over IPSec (Level 2 Tunneling Protocol over IP Security) is supported, but PPTP (Point to Point Tunneling Protocol) *is not* supported. See NAT and VPNs on Page 161.

DHCP

DHCP enables a device to be assigned a new IP address and TCP/IP parameters, including a default gateway, whenever the device reboots. Thus DHCP reduces configuration time, conserves IP addresses, and allows modules to be moved to a different network within the Cyclone system.

In conjunction with the NAT features, each SM provides

- a DHCP server that assigns IP addresses to computers connected to the SM by Ethernet protocol.
- a DHCP client that receives an IP address for the SM from a network DHCP server.

DMZ

In conjunction with the NAT features, a DMZ (demilitarized zone) allows the assignment of one IP address behind the SM for a device to logically exist outside the firewall and receive network traffic. The first three octets of this IP address must be identical to the first three octets of the NAT private IP address.

NAT Disabled

The NAT Disabled implementation is illustrated in Figure 40.

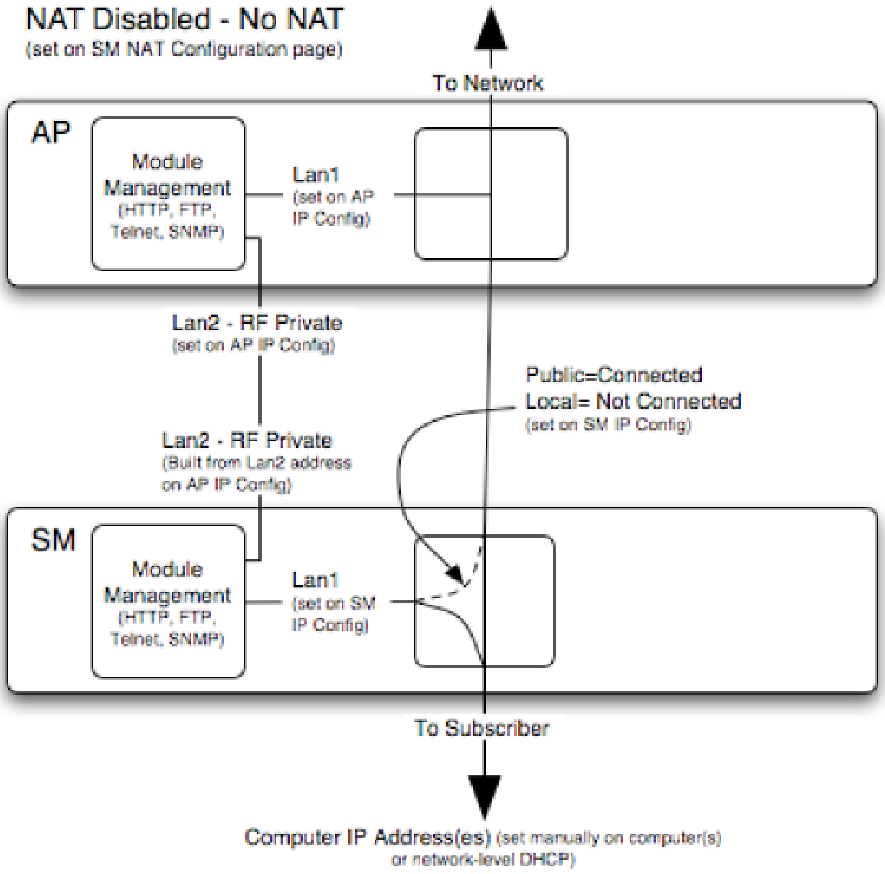

NAT Disabled - No NAT
(set on SM NAT Configuration page)
To Network
AP
Module Management (HTTP, FTP, Telnet, SNMP)
Lan1 (set on AP IP Config)
Lan2 - RF Private (set on AP IP Config)
Public=Connected
Local= Not Connected
(set on SM IP Config)
Lan2 - RF Private (Built from Lan2 address on AP IP Config)
SM
Module Management (HTTP, FTP, Telnet, SNMP)
Lan1 (set on SM IP Config)
To Subscriber
Computer IP Address(es) (set manually on computer(s) or network-level DHCP)

Figure 40: NAT Disabled implementation

NAT with DHCP Client and DHCP Server

The NAT with DHCP Client and DHCP Server implementation is illustrated in Figure 41.

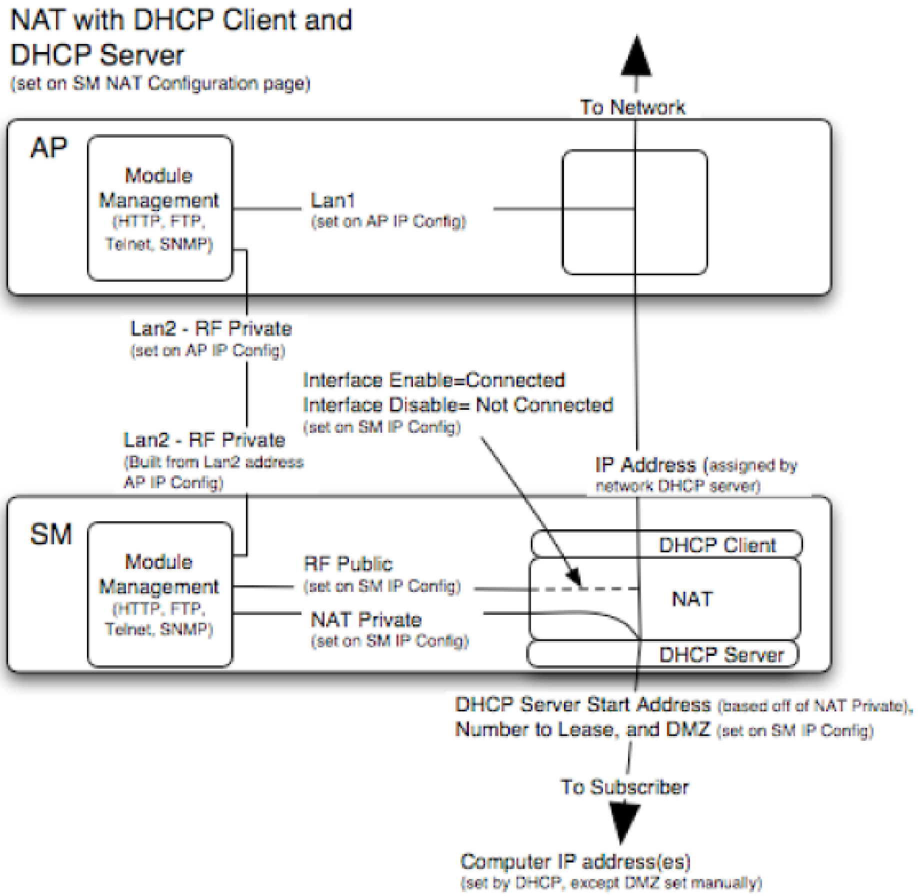

NAT with DHCP Client and DHCP Server
(set on SM NAT Configuration page)
To Network
AP
Module Management
(HTTP, FTP, Telnet, SNMP)
Lan1
(set on AP IP Config)
Lan2 - RF Private
(set on AP IP Config)
Interface Enable=Connected
Interface Disable= Not Connected
(set on SM IP Config)
Lan2 - RF Private
(Built from Lan2 address AP IP Config)
IP Address (assigned by network DHCP server)
SM
Module Management
(HTTP, FTP, Telnet, SNMP)
RF Public
(set on SM IP Config)
NAT Private
(set on SM IP Config)
DHCP Client
NAT
DHCP Server
DHCP Server Start Address (based off of NAT Private),
Number to Lease, and DMZ (set on SM IP Config)
To Subscriber
Computer IP address(es)
(set by DHCP, except DMZ set manually)

Figure 41: NAT with DHCP Client and DHCP Server implementation

NAT with DHCP Client

The NAT with DHCP Client implementation is illustrated in Figure 42.

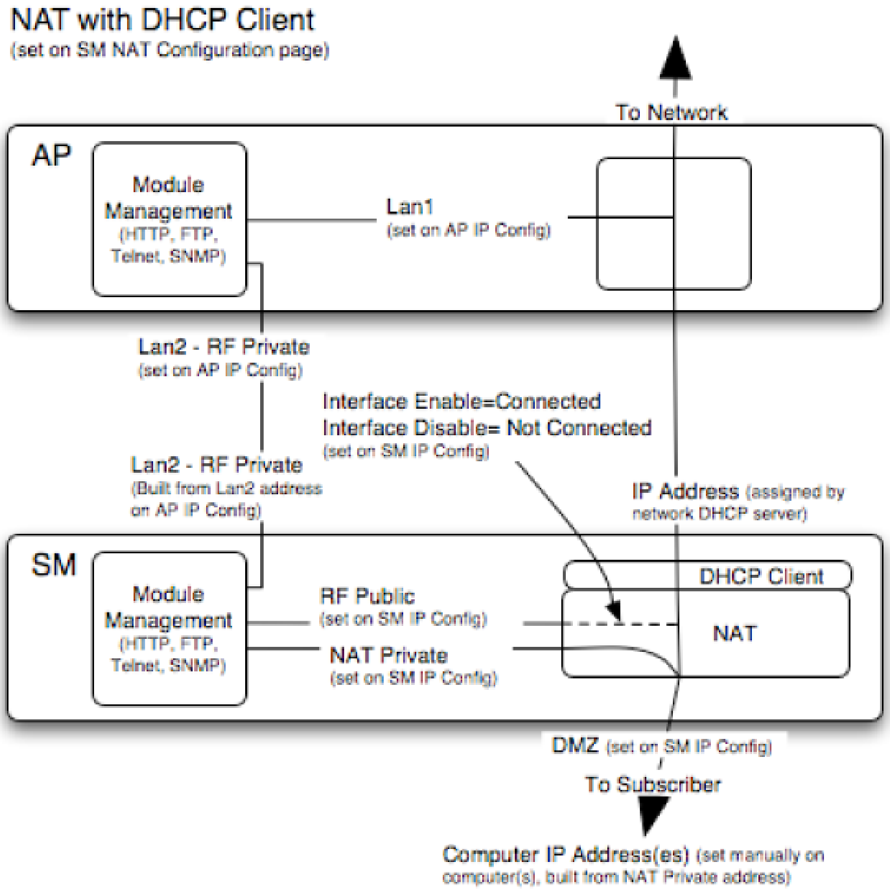

NAT with DHCP Client
(set on SM NAT Configuration page)
To Network
AP
Module Management (HTTP, FTP, Telnet, SNMP)
Lan1 (set on AP IP Config)
Lan2 - RF Private (set on AP IP Config)
Interface Enable=Connected
Interface Disable= Not Connected
(set on SM IP Config)
Lan2 - RF Private (Built from Lan2 address on AP IP Config)
IP Address (assigned by network DHCP server)
SM
Module Management (HTTP, FTP, Telnet, SNMP)
RF Public (set on SM IP Config)
NAT Private (set on SM IP Config)
DHCP Client
NAT
DMZ (set on SM IP Config)
To Subscriber
Computer IP Address(es) (set manually on computer(s), built from NAT Private address)

Figure 42: NAT with DHCP Client implementation

NAT with DHCP Server

The NAT with DHCP Server implementation is illustrated in Figure 43.

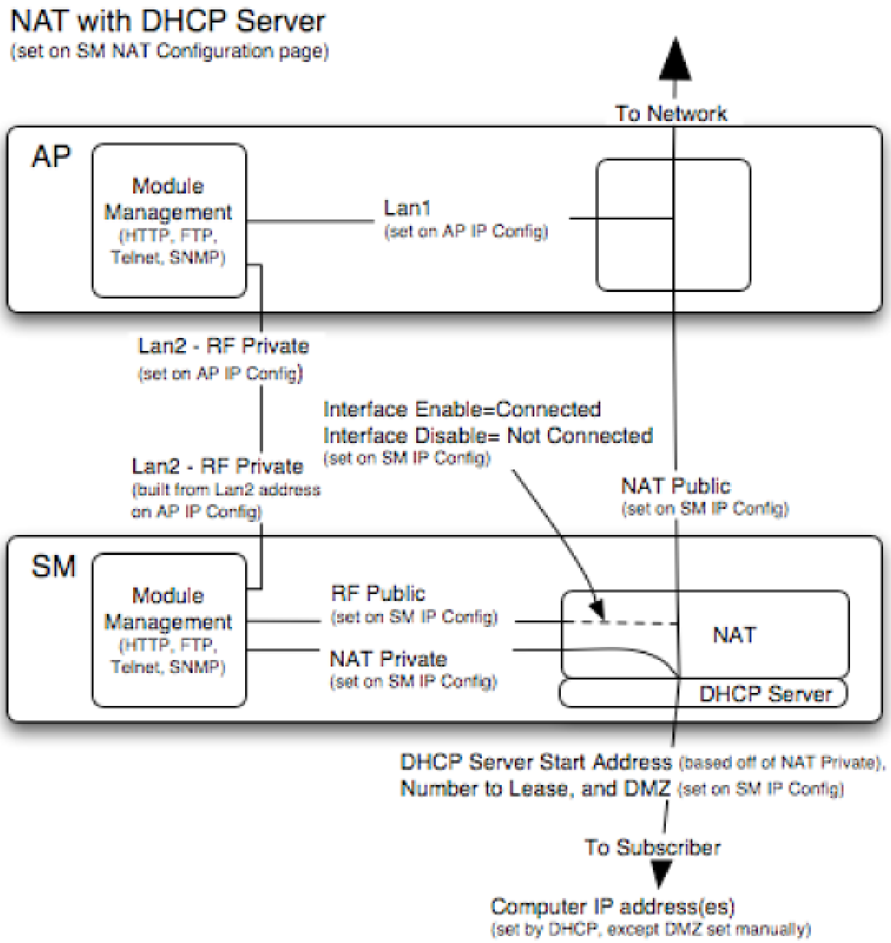

NAT with DHCP Server
(set on SM NAT Configuration page)
To Network
AP
Module Management (HTTP, FTP, Telnet, SNMP)
Lan1 (set on AP IP Config)
Lan2 - RF Private (set on AP IP Config)
Interface Enable=Connected
Interface Disable= Not Connected
(set on SM IP Config)
Lan2 - RF Private (built from Lan2 address on AP IP Config)
NAT Public (set on SM IP Config)
SM
Module Management (HTTP, FTP, Telnet, SNMP)
RF Public (set on SM IP Config)
NAT Private (set on SM IP Config)
NAT
DHCP Server
DHCP Server Start Address (based off of NAT Private),
Number to Lease, and DMZ (set on SM IP Config)
To Subscriber
Computer IP address(es)
(set by DHCP, except DMZ set manually)

Figure 43: NAT with DHCP Server implementation

NAT without DHCP

The NAT without DHCP implementation is illustrated in Figure 44.

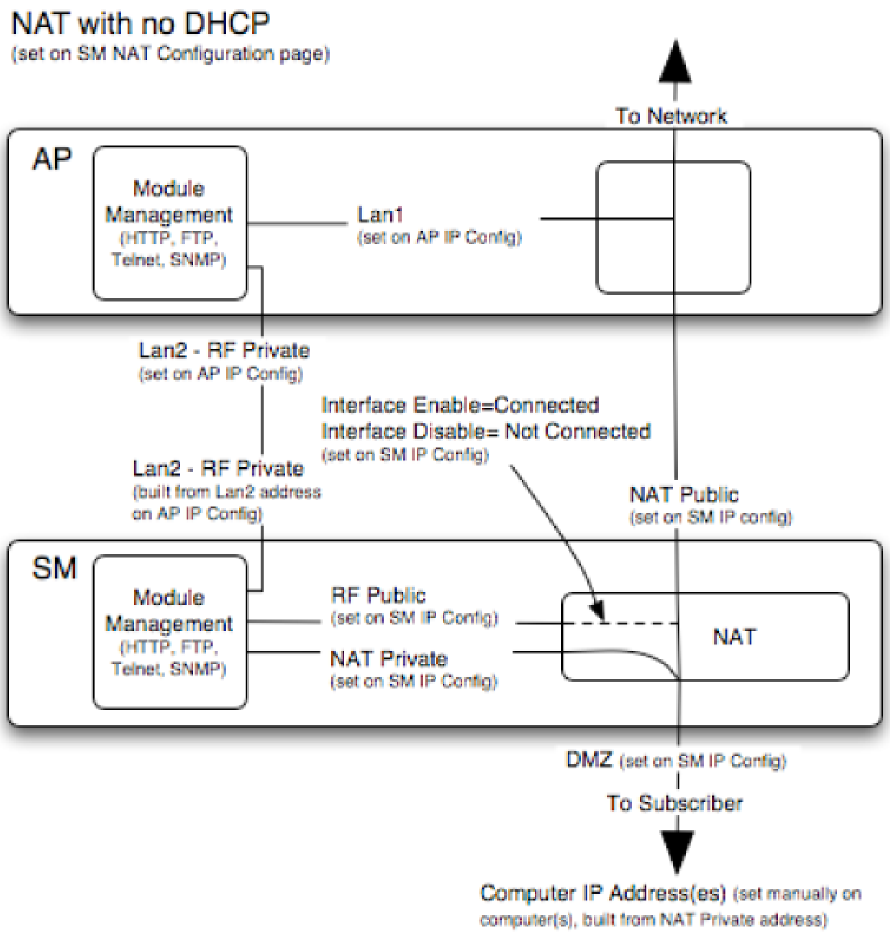

NAT with no DHCP
(set on SM NAT Configuration page)
To Network
AP
Module Management (HTTP, FTP, Telnet, SNMP)
Lan1 (set on AP IP Config)
Lan2 - RF Private (set on AP IP Config)
Interface Enable=Connected
Interface Disable= Not Connected
(set on SM IP Config)
Lan2 - RF Private (built from Lan2 address on AP IP Config)
NAT Public (set on SM IP config)
SM
Module Management (HTTP, FTP, Telnet, SNMP)
RF Public (set on SM IP Config)
NAT Private (set on SM IP Config)
NAT
DMZ (set on SM IP Config)
To Subscriber
Computer IP Address(es) (set manually on computer(s), built from NAT Private address)

Figure 44: NAT without DHCP implementation

13.3.2 NAT and VPNs

VPN technology provides the benefits of a private network during communication over a public network. One typical use of a VPN is to connect remote employees, who are at home or in a different city, to their corporate network over the public Internet. Any of several VPN implementation schemes is possible. By design, NAT translates or changes addresses, and thus interferes with a VPN that is not specifically supported by a given NAT implementation.

With NAT enabled, SMs support L2TP over IPSec (Level 2 Tunneling Protocol over IP Security) VPNs, but *do not* support PPTP (Point to Point Tunneling Protocol) VPNs. With NAT disabled, SMs support all types of VPNs.

13.4 DEVELOPING AN IP ADDRESSING SCHEME

Cyclone network elements are accessed through IP Version 4 (IPv4) addressing. A proper IP addressing method is critical to the operation and security of a Cyclone network.

Each Cyclone module requires an IP address on the network. This IP address is for only management purposes. For security, you should either

- assign an unroutable IP address.
- assign a routable IP address only if a firewall is present to protect the module.

You will assign IP addresses to computers and network components by either *static* or *dynamic* IP addressing. You will also assign the appropriate subnet mask and network gateway to each module.

13.4.1 Address Resolution Protocol

As previously stated, the MAC address identifies a Cyclone module in

- communications between modules.
- the data that modules store about each other.
- the data that BAM or Prizm applies to manage authentication and bandwidth.

The IP address is essential for data delivery through a router interface. Address Resolution Protocol (ARP) correlates MAC addresses to IP addresses.

For communications to outside the network segment, ARP reads the network gateway address of the router and translates it into the MAC address of the router. Then the communication is sent to MAC address (physical network interface card) of the router.

For each router between the sending module and the destination, this sequence applies. The ARP correlation is stored until the ARP cache times out.

13.4.2 Allocating Subnets

The subnet mask is a 32-bit binary number that filters the IP address. Where a subnet mask contains a bit set to 1, the corresponding bit in the IP address is part of the network address.

Example IP Address and Subnet Mask

In Figure 45, the first 16 bits of the 32-bit IP address identify the network:

	Octet 1	**Octet 2**	**Octet 3**	**Octet 4**
IP address 169.254.1.1	10101001	11111110	00000001	00000001
Subnet mask 255.255.0.0	11111111	11111111	00000000	00000000

Figure 45: Example of IP address in Class B subnet

In this example, the network address is 169.254, and 2^{16} (65,536) hosts are addressable.

13.4.3 Selecting Non-routable IP Addresses

The factory default assignments for Cyclone network elements are

- unique MAC address
- IP address of 169.254.1.1, except for an OFDM series BHM, whose IP address is 169.254.1.2 by default
- subnet mask of 255.255.0.0
- network gateway address of 169.254.0.0

For each Cyclone radio and CMMmicro, assign an IP address that is both consistent with the IP addressing plan for your network and cannot be accessed from the Internet. IP addresses within the following ranges are not routable from the Internet, regardless of whether a firewall is configured:

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

You can also assign a subnet mask and network gateway for each CMMmicro.

14 ENGINEERING VLANS

Cyclone radios support VLAN functionality as defined in the 802.1Q (*Virtual LANs*) specification, except for the following aspects of that specification:

- the following protocols:
  - Generic Attribute Registration Protocol (GARP) GARV
  - Spanning Tree Protocol (STP)
  - Multiple Spanning Tree Protocol (MSTP)
  - GARP Multicast Registration Protocol (GMRP)
- priority encoding (802.1P) before Release 7.0
- embedded source routing (ERIF) in the 802.1Q header
- multicast pruning
- flooding unknown unicast frames in the downlink

As an additional exception, the Cyclone AP *does not* flood downward the unknown unicast frames to the Canopy SM.

A VLAN configuration in Layer 2 establishes a logical group within the network. Each computer in the VLAN, regardless of initial or eventual physical location, has access to the same data. For the network operator, this provides flexibility in network segmentation, simpler management, and enhanced security.

14.1 SM MEMBERSHIP IN VLANS

With the supported VLAN functionality, Cyclone radios determine bridge forwarding on the basis of not only the destination MAC address, but also the VLAN ID of the destination. This provides flexibility in how SMs are used:

- Each SM can be a member in its own VLAN.
- Each SM can be in its own broadcast domain, such that only the radios that are members of the VLAN can see broadcast and multicast traffic to and from the SM.
- The network operator can define a work group of SMs, regardless of the AP(s) to which they register.

Cyclone point-to-multipoint modules provide the VLAN frame filters that are described in Table 36.

Table 36: VLAN filters in point-to-multipoint modules

Where VLAN is active, if this parameter value is selected …	**then a frame is discarded if…**		**because of this VLAN filter in the Cyclone software:**
	***entering* the bridge/ NAT switch through…**		
	Ethernet…	**TCP/IP…**	
any combination of VLAN parameter settings	with a VID not in the membership table		Ingress
any combination of VLAN parameter settings		with a VID not in the membership table	Local Ingress
Allow Frame Types: Tagged Frames Only	with no 802.1Q tag		Only Tagged
Allow Frame Types: Untagged Frames Only	with an 802.1Q tag, regardless of VID		Only Untagged
Local SM Management: Disable in the SM, or **All Local SM Management: Disable** in the AP	with an 802.1Q tag and a VID in the membership table		Local SM Management
	***leaving* the bridge/ NAT switch through…**		
	Ethernet…	**TCP/IP…**	
any combination of VLAN parameter settings	with a VID not in the membership table		Egress
any combination of VLAN parameter settings		with a VID not in the membership table	Local Egress

14.2 PRIORITY ON VLANS (802.1p)

Cyclone radios can prioritize traffic based on the eight priorities described in the IEEE 802.1p specification. When the high-priority channel is enabled on an SM, regardless of whether VLAN is enabled on the AP for the sector, packets received with a priority of 4 through 7 in the 802.1p field are forwarded onto the high-priority channel.

VLAN settings in a Cyclone module can also cause the module to convert received non-VLAN packets into VLAN packets. In this case, the 802.1p priority in packets leaving the module is set to the priority established by the DiffServ configuration.

If you enable VLAN, *immediately* monitor traffic to ensure that the results are as desired. For example, high-priority traffic may block low-priority.

For more information on the Cyclone high priority channel, see High-priority Bandwidth on Page 86.

Installation and Configuration Guide

15 AVOIDING HAZARDS

Use simple precautions to protect staff and equipment. Hazards include exposure to RF waves, lightning strikes, and power surges. This section specifically recommends actions to abate these hazards.

15.1 EXPOSURE SEPARATION DISTANCES

To protect from overexposure to RF energy, install Cyclone radios so as to provide and maintain the minimum separation distances from all persons shown in Table 37.

Table 37: Exposure separation distances

Module Type	Separation Distance from Persons
Cyclone Module, FSK or OFDM	At least 20 cm (approx 8 in)
Cyclone Module with Reflector Dish	At least 1.5 m (approx 60 in or 5 ft)
Cyclone Module with LENS	At least 0.5 m (approx 20 in)
Antenna of connectorized 5.7 GHz AP	At least 30 cm (approx 12 in)
Antenna of connectorized or integrated 900 MHz module	At least 60 sm (24 in)
Indoor 900 MHz SM	At least 10 cm (4 in)

Section 15.1.1 and Table 38 give details and discussion of the associated calculations.

15.1.1 Details of Exposure Separation Distances Calculations and Power Compliance Margins

Limits and guidelines for RF exposure come from:

- US FCC limits for the general population. See the FCC web site at http://www.fcc.gov, and the policies, guidelines, and requirements in Part 1 of Title 47 of the Code of Federal Regulations, as well as the guidelines and suggestions for evaluating compliance in FCC OET Bulletin 65.
- Health Canada limits for the general population. See the Health Canada web site at http://www.hc-sc.gc.ca/rpb and Safety Code 6.
- ICNIRP (International Commission on Non-Ionizing Radiation Protection) guidelines for the general public. See the ICNIRP web site at http://www.icnirp.de/ and Guidelines for Limiting Exposure to Time-Varying Electric, Magnetic, and Electromagnetic Fields.

The applicable power density exposure limits from the documents referenced above are

- 6 W/m^2 for RF energy in the 900-MHz frequency band in the US and Canada.
- 10 W/m^2 for RF energy in the 2.4-, 5.2-, 5.4-, and 5.7-GHz frequency bands.

Peak power density in the far field of a radio frequency point source is calculated as follows:

$$S = \frac{P \cdot G}{4\,\pi\,d^2}$$

where
S = power density in W/m^2
P = RMS transmit power capability of the radio, in W
G = total Tx gain as a factor, converted from dB
d = distance from point source, in m

Rearranging terms to solve for distance yields

$$d = \sqrt{\frac{P \cdot G}{4\,\pi\,S}}$$

Table 38 shows calculated minimum separation distances *d*, recommended distances and resulting power compliance margins for each frequency band and antenna combination.

Table 38: Calculated exposure distances and power compliance margins

Frequency Band	**Antenna**	**Variable**			***d*** **(calculated)**	**Recommended Separation Distance**	**Power Compliance Margin**
		P	**G**	**S**			
900 MHz	external	0.4 W (26 dBm)	10.0 (10 dB)	6 W/m^2	23 cm	60 cm (24 in)	7
	integrated	0.25 W (24 dBm)	15.8 (12 dB)	6 W/m^2	23 cm	60 cm (24 in)	7
	indoor, integrated	Simulation model used to estimate Specific Absorption Rate (SAR) levels				10 cm (4 in)	2
2.4 GHz	integrated	0.34 W (25 dBm)	6.3 (8 dB)	10 W/m^2	13 cm	20 cm (8 in)	2.3
	integrated plus reflector	0.34 W (25 dBm)	79.4 (19 dB)	10 W/m^2	46 cm	1.5 m (5 ft)	10
5.2 GHz	integrated	0.2 W (23 dBm)	5.0 (7 dB)	10 W/m^2	9 cm	20 cm (8 in)	5
	integrated plus reflector	0.0032 W (5 dBm)	316 (25 dB)	10 W/m^2	9 cm	1.5 m (5 ft)	279
	integrated plus LENS	0.025 W (14 dBm)	40 (16 dB)	10 W/m^2	9 cm	50 cm (12 in)	31
5.4 GHz	integrated	0.2 W (23 dBm)	5.0 (7 dB)	10 W/m^2	9 cm	20 cm (8 in)	5
	integrated plus reflector	0.0032 W (5 dBm)	316 (25 dB)	10 W/m^2	9 cm	1.5 m (5 ft)	279
	integrated plus LENS	0.020 W (13 dBm)	50 (17 dB)	10 W/m^2	9 cm	50 cm (12 in)	31
5.4 GHz OFDM	integrated	0.01 W (10 dBm)	50 (17 db)	10 W/m^2	6 cm	20 cm (8 in)	10

Frequency Band	**Antenna**	**Variable**			***d*** **(calculated)**	**Recommended Separation Distance**	**Power Compliance Margin**
		P	***G***	***S***			
5.7 GHz	integrated	0.2 W (23 dBm)	5.0 (7 dB)	10 W/m^2	9 cm	20 cm (8 in)	5
	integrated plus reflector	0.2 W (23 dBm)	316 (25 dB)	10 W/m^2	71 cm	1.5 m (5 ft)	4.5
	Integrated plus LENS	0.2 W (23 dBm)	50 (17 dB)	1 W/m^2	28 cm	50 cm (12 in)	3.13

The “Recommended Distances” are chosen to give significant compliance margin in all cases. They are also chosen so that a given item (bare module, reflector, or LENS) always has the same distance, regardless of frequency band, to simplify following exposure distances in the field.

These are conservative distances:

- They are along the beam direction (the direction of greatest energy). Exposure to the sides and back of the module will be significantly less.
- They meet sustained exposure limits for the general population (not just short term occupational exposure limits), with considerable margin.
- In the reflector cases, the calculated compliance distance *d* is greatly overestimated because the far-field equation models the reflector as a point source and neglects the physical dimension of the reflector.

15.2 GROUNDING CYCLONE EQUIPMENT

Effective lightning protection diverts lightning current safely to ground, Protective Earth (PE) ⏚. It neither attracts nor prevents lightning strikes.

> ***WARNING!***
> Lightning damage *is not* covered under the Cyclone warranty. The recommendations in Cyclone guides give the installer the knowledge to protect the installation from the harmful effects of ESD and lightning. These recommendation must be thoroughly and correctly performed. However, complete protection is neither implied or possible.

15.2.1 Grounding Infrastructure Equipment

To protect both your staff and your infrastructure equipment, implement lightning protection as follows:

- Observe all local and national codes that apply to grounding for lightning protection.
- Before you install your Cyclone modules, perform the following steps:
    - Engage a grounding professional if you need to do so.

  - Install lightning arrestors to transport lightning strikes away from equipment. For example, install a lightning rod on a tower leg other than the leg to which you mount your module.
  - Connect your lightning rod to ground.
  - Use a Cyclone 600SS Surge Suppressor on the Ethernet cable where the cable enters any structure. (Instructions for installing a Cyclone 600SS Surge Suppressor are provided in Procedure 28 on Page 349.)
- Install your modules at least 2 feet (0.6 meters) below the tallest point on the tower, pole, or roof.

15.2.2 Grounding SMs

This section provides lightning protection guidelines for SMs to satisfy the National Electrical Code (NEC) of the United States. The requirements of the NEC focus on the safety aspects of electrical shock to personnel and on minimizing the risk of fire at a dwelling. The NEC does not address the survivability of electronic products that are exposed to lightning surges.

The statistical incidence of current levels from lightning strikes is summarized in Table 39.

Table 39: Statistical incidence of current from lightning strikes

Percentage of all strikes	Peak Current (amps)
<2	>140,000
25	>35,000
>50	>20,000
>80	>8,500

At peak, more than one-half of all surges due to direct lightning strikes exceed 20,000 amps. However, only one-quarter exceed 35,000 amps, and less than two percent exceed 140,000 amps. Thus, the recommended Surge Suppressor (300SS) provides a degree of lightning protection to electronic devices inside a dwelling.

Summary of Grounding Recommendations

Last Mile Gear recommends that you ground each SM as follows:

- Extend the SM mounting bracket extend to the top of the SM or higher.
- Ground the SM mounting bracket via a 10-AWG (6 mm^2) copper wire connected by the most direct path either to an eight foot-deep ground rod or to the ground bonding point of the AC power service utility entry. This provides the best assurance that
  - lightning takes the ground wire route
  - the ground wire does not fuse open
  - your grounding system complies with NEC 810-15.
- Ground the Cyclone Surge Suppressor 300SS or 600SS ground lug to the same ground bonding point as above, using at least a 10-AWG (6 mm^2) copper wire. This provides the best assurance that your grounding system complies with NEC 810-21.

Grounding Scheme

The proper overall antenna grounding scheme per the NEC is illustrated in Figure 128 on Page 350. In most television antenna or dish installations, a coaxial cable connects the outdoor electronics with the indoor electronics. To meet NEC 810-20, one typically uses a coaxial cable feed-through block that connects the outdoor coax to the indoor coax and also has a screw for attaching a ground wire. This effectively grounds the outer shield of the coax. The block should be mounted on the outside of the building near the AC main panel such that the ground wire of the block can be bonded to the primary grounding electrode system of the structure.

For residential installs, in most cases an outdoor rated *un*shielded twisted pair (UTP) cable is sufficient. To comply with the NEC, Last Mile Gear provides the antenna discharge unit, 300SS or 600SS, for each conductor of the cable. The surge suppressor must be

- ◦ positioned
    - outside the building.
    - as near as practicable to the power service entry panel of the building and attached to the AC main power ground electrode, or attached to a grounded water pipe.[5]
    - far from combustible material.
- ◦ grounded in accordance with NEC 810-21, with the grounding wire attached to the screw terminal.

The metal structural elements of the antenna mast also require a separate grounding conductor. Section 810-15 of the NEC states:

> *Masts and metal structures supporting antennas shall be grounded in accordance with Section 810-21.*

As shown in Figure 128 on Page 350, the Last Mile Gear recommendation for grounding the metal structural element of the Cyclone mounting bracket (SMMB1) is to route the grounding wire from the SMMB1 down to the same ground attachment point as is used for the 300SS discharge unit.

Use 10-AWG (6 mm^2) Copper Grounding Wire

According to NEC 810-21 3(h), either a 16-AWG copper clad steel wire or a 10-AWG copper wire may be used. This specification appears to be based on mechanical strength considerations and *not* on lightning current handling capabilities.

For example, analysis shows that the two wire types are not equivalent when carrying a lightning surge that has a 1-microsecond rise by 65-microsecond fall:

- ◦ The 16-AWG copper clad steel wire has a peak fusing current of 35,000 amps and can carry 21,000 amps peak, at a temperature just below the ignition point for paper (454° F or 234° C).
- ◦ The 10-AWG copper wire has a peak fusing current of 220,000 amps and can carry 133,000 amps peak, at the same temperature.

[5] It is *insufficient* to merely use the green wire ground in a duplex electrical outlet box for grounding of the antenna discharge unit.

Based on the electrical/thermal analysis of these wires, Last Mile Gear recommends 10-AWG copper wire for *all* grounding conductors. Although roughly double the cost of 16-AWG copper clad steel wire, 10-AWG copper wire handles six times the surge current from lightning.

Shielding is not Grounding

In part, NEC 810-21 states:

> *A lightning arrester is not required if the lead-in conductors are enclosed in a continuous metal shield, such as rigid or intermediate metal conduit, electrical metallic tubing, or any metal raceway or metal-shielded cable that is effectively grounded. A lightning discharge will take the path of lower impedance and jump from the lead-in conductors to the metal raceway or shield rather than take the path through the antenna coil of the receiver.*

However, Last Mile Gear does not recommend relying on shielded twisted pair cable for lightning protection for the following reasons:

- Braid-shielded 10Base-T cable is uncommon, if existent, and may be unsuitable anyway.
- At a cost of about two-thirds more than 10-AWG copper UTP, CAT 5 100Base-TX foil-shielded twisted pair (FTP) cable provides a 24-AWG drain wire. If this wire melts open during a lightning surge, then the current may follow the twisted pair into the building.

  More than 80 percent of all direct lightning strikes have current that exceeds 8,500 amps (see Table 39 on Page 172). A 24-AWG copper wire melts open at 8,500 amps from a surge that has a 1-microsecond by 70-microsecond waveform. Hence, reliance on 24-AWG drain wire to comply with the intent of NEC 810-21 is questionable.

Shielded twisted pair cable may be useful for mitigation of interference in some circumstances, but installing surge suppressors and implementing the ground recommendations constitute the most effective mitigation against lightning damage.

NEC Reference

NEC Article 810, *Radio and Television Equipment*, and associated documents and discussions are available from http://www.neccode.com/index.php?id=homegeneral, http://www.constructionbook.com/xq/ASP/national-electrical-code-2005/id.370/subID.746/qx/default2.htm, and other sources.

15.3 CONFORMING TO REGULATIONS

For all electrical purposes, ensure that your network conforms to applicable country and local codes, such as the NEC (National Electrical Code) in the US. If you are uncertain of code requirements, engage the services of a licensed electrician.

15.4 PROTECTING CABLES AND CONNECTIONS

Cables that move in the wind can be damaged, impart vibrations to the connected device, or both. At installation time, prevent these problems by securing all cables with cable ties, cleats, or PVC tape.

Over time, moisture can cause a cable connector to fail. You can prevent this problem by

- using cables that are filled with a dielectric gel or grease.
- including a drip loop where the cable approach to the module (typically a CMM2 or CMMmicro) is from above.
- wrapping the cable with weather-resistant tape.

On a module with an external antenna, use accepted industry practices to wrap the connector to prevent water ingress. Although the male and female N-type connectors form a gas-tight seal with each other, the point where the cable enters each connector can allow water ingress and eventual corrosion. Wrapping and sealing is critical to long-term reliability of the connection.

Possible sources of material to seal that point include

- the antenna manufacturer (material may have been provided in the package with the antenna).
- Universal Electronics (whose web site is http://www.coaxseal.com), who markets a weather-tight wrap named Coax-Seal.

Perform the following steps to wrap the cable.

Procedure 4: Wrapping the cable

1. Start the wrap on the cable 0.5 to 2 inches (about 1.5 to 5 cm) from the connection.
2. Wrap the cable to a point 0.5 to 2 inches (about 1.5 to 5 cm) above the connection.
3. Squeeze the wrap to compress and remove any trapped air.
4. Wrap premium vinyl electrical tape over the first wrap where desired for abrasion resistance or appearance.
5. Tie the cable to minimize sway from wind.

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

16 TESTING THE COMPONENTS

The best practice is to connect all components—BHs, APs, GPS antenna, and CMM2 or CMMmicro—in a test setting and initially configure and verify them before deploying them to an installation. In this way, any configuration issues are worked out before going on-site, on a tower, in the weather, where the discovery of configuration issues or marginal hardware is more problematic and work-flow affecting.

16.1 UNPACKING COMPONENTS

When you receive Cyclone products, carefully inspect all shipping boxes for signs of damage. If you find damage, immediately notify the transportation company.

As you unpack the equipment, verify that all the components that you ordered have arrived. Save all the packing materials to use later, as you transport the equipment to and from installation sites.

16.2 CONFIGURING FOR TEST

You can use either of two methods to configure an AP or BHM:

- Use the Quick Start feature of the product. For more information on Quick Start, see Quick Start Page of the AP on Page 185.
- Manually set each parameter.

After you change configuration parameters on a GUI web page:

1. Before you leave a web page, click the **Save** button to save the change(s).
2. After making change(s) on multiple web pages, click the **Reboot** button to reboot the module and implement the change(s).

16.2.1 Configuring the Computing Device for Test

If your computer is configured for Dynamic Host Configuration Protocol (DHCP), disconnect the computer from the network. If your computer is instead configured for static IP addressing

- set the static address in the 169.254 network
- set the subnet mask to 255.255.0.0.

16.2.2 Default Module Configuration

From the factory, the Cyclone AP, SM, and BH are all configured to *not transmit* on any frequency. This configuration ensures that you do not accidentally turn on an unsynchronized module. Site synchronization of modules is required because

- Cyclone modules
  - cannot transmit and receive signals at the same time.
  - use TDD (Time Division Duplexing) to distribute signal access of the downlink and uplink frames.
- when one module transmits while an unintended module nearby receives signal, the transmitting module may interfere with or desense the receiving module. In this context, interference is self-interference (within the same Cyclone network).

16.2.3 Component Layout

As shown in Figure 46, the base cover of the module snaps off when you depress a lever on the back of the base cover. This exposes the Ethernet and GPS sync connectors and diagnostic LEDs.

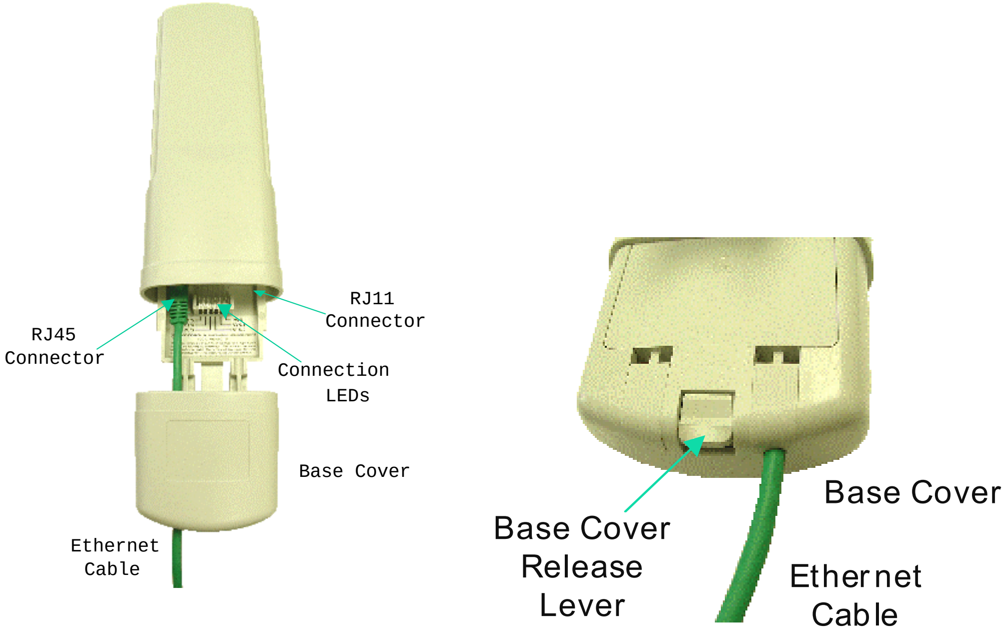


Figure 46: Cyclone base cover, attached and detached

16.2.4 Diagnostic LEDs

The diagnostic LEDs report the following information about the status of the module. Table 40 and Table 41 identify the LEDs in order of their left-to-right position as the cable connections face downward.

> *NOTE:*
> The LED color helps you distinguish position of the LED. The LED color *does not* indicate any status.

Table 40: LEDs in AP and BHM

Label	Color when Active	Status Information Provided	Notes
LNK/5	green	Ethernet link	Continuously lit when link is present.
ACT/4	orange	Presence of data activity on the Ethernet link	Flashes during data transfer. Frequency of flash is not a diagnostic indication.
GPS/3	red	Pulse of sync	Continuously lit as pulse as AP receives pulse.
SES/2	green	*Unused on the AP*	SES is the session indicator on the CMM.
SYN/1	orange	Presence of sync	Always lit on the AP.
PWR	red	DC power	Always lit when power is correctly supplied.

Table 41: LEDs in SM and BHS

Label	Color when Active	Status if Registered	Notes	
			Operating Mode	Aiming Mode
LNK/5	green	Ethernet link	Continuously lit when link is present.	These five LEDs act as a bar graph to indicate the relative quality of alignment. As power level and jitter improve during alignment, more of these LEDs are lit.
ACT/4	orange	Presence of data activity on the Ethernet link	Flashes during data transfer. Frequency of flash is not a diagnostic indication.	
GPS/3	red	*Unused*	If this module is not registered to another, then these three LEDs cycle on and off from left to right.	
SES/2	green	*Unused*		
SYN/1	orange	Presence of sync		
PWR	red	DC power	Always lit when power is correctly supplied.	Always lit when power is correctly supplied.

16.2.5 CMM2 Component Layout

As shown in Figure 125 on Page 344, the CMM2 comprises four assemblies:

- Ethernet switch
- Power transformer
- Interconnect board
- GPS receiver.

Some CMM2s that were sold earlier had four openings in the bottom plate, as shown in Figure 47. Currently available CMM2s have two *additional* Ethernet cable and GPS sync cable openings to allow use of thicker, shielded cables.

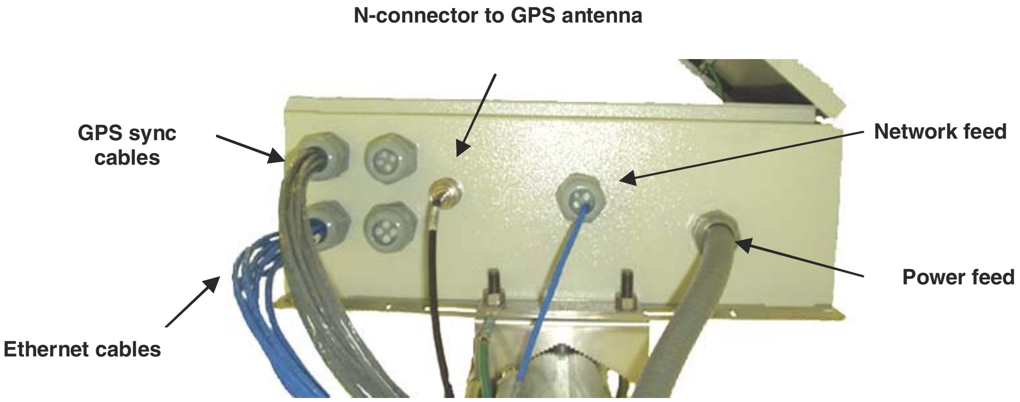
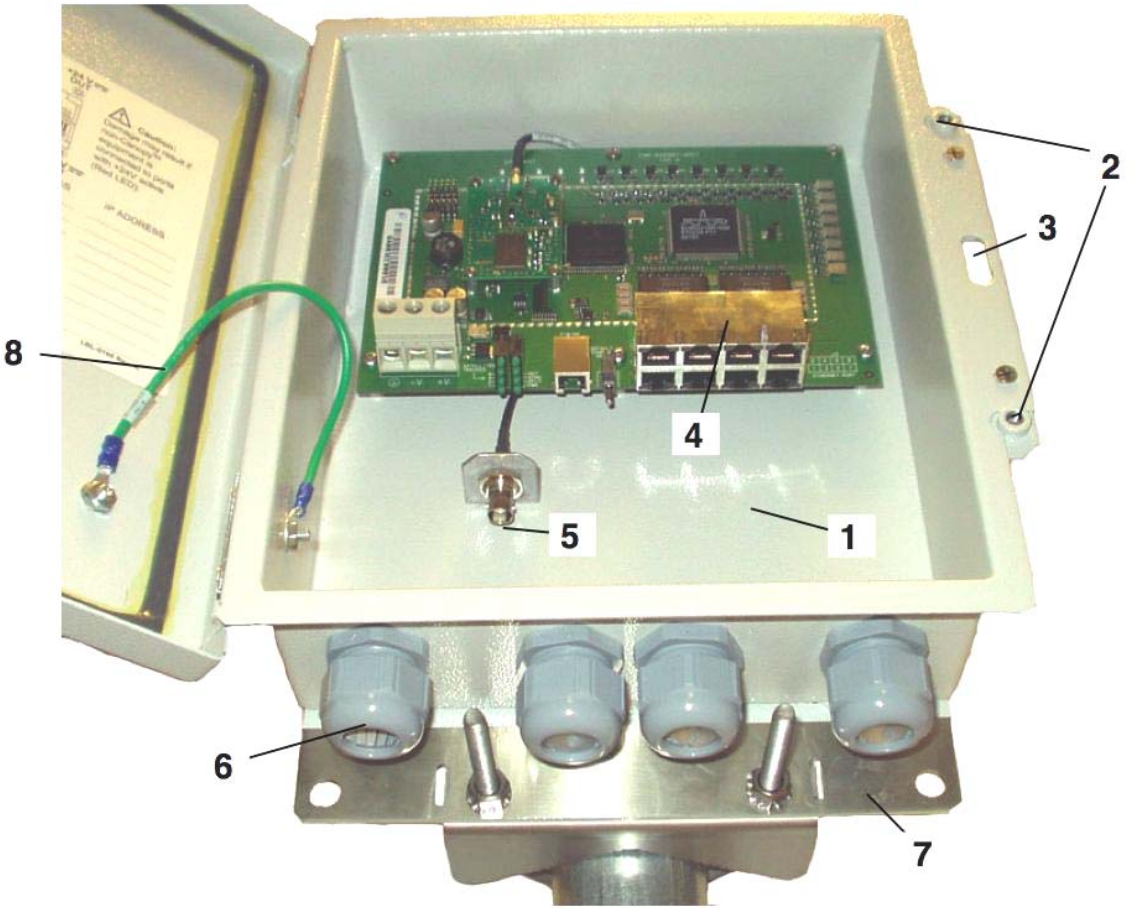


Figure 47: Cyclone CMM2, bottom view

16.2.6 CMMmicro Component Layout

The layout of the CMMmicro is shown in Figure 48.



LEGEND

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 for grounding to tower or building) using U bolts (provided) or other hardware such as screws, lag bolts, or attachment straps (not provided)
8. Ground strap (for grounding door to enclosure)
9. 100-W 115/230-V AC to 24-V DC power converter, with 10 ft (3 m) of DC power cable (not shown)
10. 6-ft (1.8-m) AC power cord for 24 V power converter (not shown)

Figure 48: Cluster Management Module micro

16.2.7 Standards for Wiring

Cyclone modules automatically sense whether the Ethernet cable in a connection is wired as straight-through or crossover. You may use either straight-through or crossover cable to connect a network interface card (NIC), hub, router, or switch to these modules. For a straight-through cable, use the EIA/TIA-568B wire color-code standard on both ends. For a crossover cable, use the EIA/TIA-568B wire color-code standard on one end, and the EIA/TIA-568A wire color-code standard on the other end.

Where you use the Cyclone AC wall adapter

- the power supply output is +24 VDC.
- the power input to the SM is +11.5 VDC to +30 VDC.
- the maximum Ethernet cable run is 328 feet (100 meters).

16.2.8 Best Practices for Cabling

The following practices are essential to the reliability and longevity of cabled connections:

- Use only shielded cables to resist interference.
- For vertical runs, provide cable support and strain relief.
- Include a 2-ft (0.6-m) service loop on each end of the cable to allow for thermal expansion and contraction and to facilitate terminating the cable again when needed.
- Include a drip loop to shed water so that most of the water does not reach the connector at the device.
- Properly crimp all connectors.
- Use dielectric grease on all connectors to resist corrosion.
- Use only shielded connectors to resist interference and corrosion.

16.2.9 Recommended Tools for Wiring Connectors

The following tools may be needed for cabling the AP:

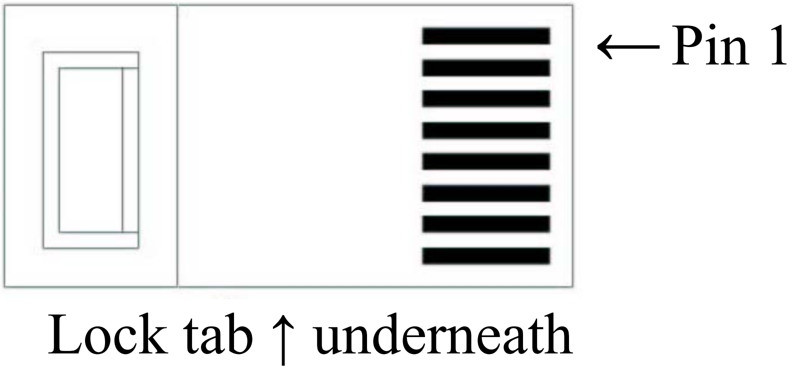
- RJ-11 crimping tool
- RJ-45 crimping tool
- electrician scissors
- wire cutters
- cable testing device.

16.2.10 Wiring Connectors

The following diagrams correlate pins to wire colors and illustrate crossovers where applicable.

Location of Pin 1

Pin 1, relative to the lock tab on the connector of a straight-through cable is located as shown below.



RJ-45 Pinout for Straight-through Ethernet Cable

Pin 1 →	white / orange	← Pin 1
Pin 2 →	orange	← Pin 2
Pin 3 →	white / green	← Pin 3
Pin 4 →	blue	← Pin 4
Pin 5 →	white / blue	← Pin 5
Pin 6 →	green	← Pin 6
Pin 7 →	white / brown	← Pin 7
Pin 8 →	brown	← Pin 8

Pins 7 and 8 carry power to the modules.

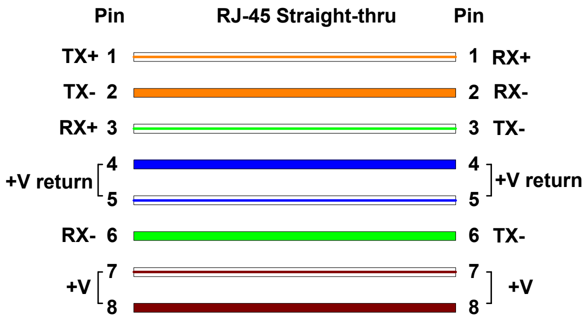


Figure 49: RJ-45 pinout for straight-through Ethernet cable

RJ-45 Pinout for Crossover Ethernet Cable

Pin 1 →	white / orange	← Pin 3
Pin 2 →	orange	← Pin 6
Pin 3 →	white / green	← Pin 1
Pin 4 →	blue	← Pin 4
Pin 5 →	white / blue	← Pin 5
Pin 6 →	green	← Pin 2
Pin 7 →	white / brown	← Pin 7
Pin 8 →	brown	← Pin 8

Pins 7 and 8 carry power to the modules.

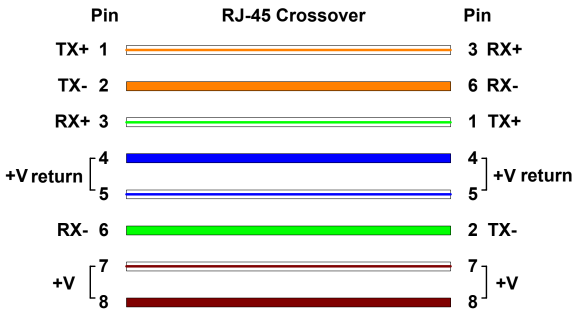


Figure 50: RJ-45 pinout for crossover Ethernet cable

RJ-11 Pinout for Straight-through Sync Cable

The Cyclone system uses a utility cable with RJ-11 connectors between the AP or BH and synchronization pulse. Presuming CAT 5 cable and 6-pin RJ-11 connectors, the following diagram shows the wiring of the cable for sync.

Pin 1 → white / orange ← Pin 1
Pin 2 → white / green ← Pin 2
Pin 3 → white / blue ← Pin 3
Pin 4 → green ← Pin 4
Pin 5 → blue ← Pin 5
Pin 6 → orange ← Pin 6
NOTE: The fourth pair is not used.

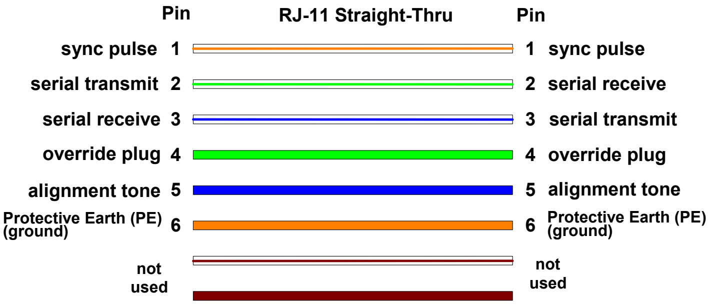


Figure 51: RJ-11 pinout for straight-through sync cable

16.2.11 Alignment Tone—Technical Details

The alignment tone output from a Cyclone module is available on Pin 5 of the RJ-11 connector, and ground is available on Pin 6. Thus the load at the listening device should be between Pins 5 and 6. The listening device may be a headset, earpiece, or battery-powered speaker.

16.3 CONFIGURING A POINT-TO-MULTIPOINT LINK FOR TEST

Perform the following steps to begin the test setup.

Procedure 5: Setting up the AP for Quick Start

1. In one hand, securely hold the top (larger shell) of the AP. 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 AP.
3. Plug the Ethernet cable connector labeled To Radio into the jack in the pig tail that hangs from the power supply.

WARNING!
From this point until you remove power from the AP, stay at least as far from the AP as the minimum separation distance specified in Table 37 on Page 169.

4. Plug the other connector of the pig tail (this connector labeled To Computer) into the Ethernet jack of the computing device.
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 Cyclone AP interface provides a series of web pages to configure and monitor the unit. You can access the web-based interface through a computing device that is either directly connected or connected through a network to the AP. 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 Cyclone module, then you may need to first disable the proxy setting in the computer.

Perform the following procedure to toggle the computer to *not* use the proxy setting.

Procedure 6: Bypassing proxy settings to access module web pages

1. Launch Microsoft Internet Explorer.
2. Select **Tools→Internet Options→Connections→LAN Settings**.
3. Uncheck the **Use a proxy server…** box.
   NOTE: If you use an alternate web browser, the menu selections differ from the above.

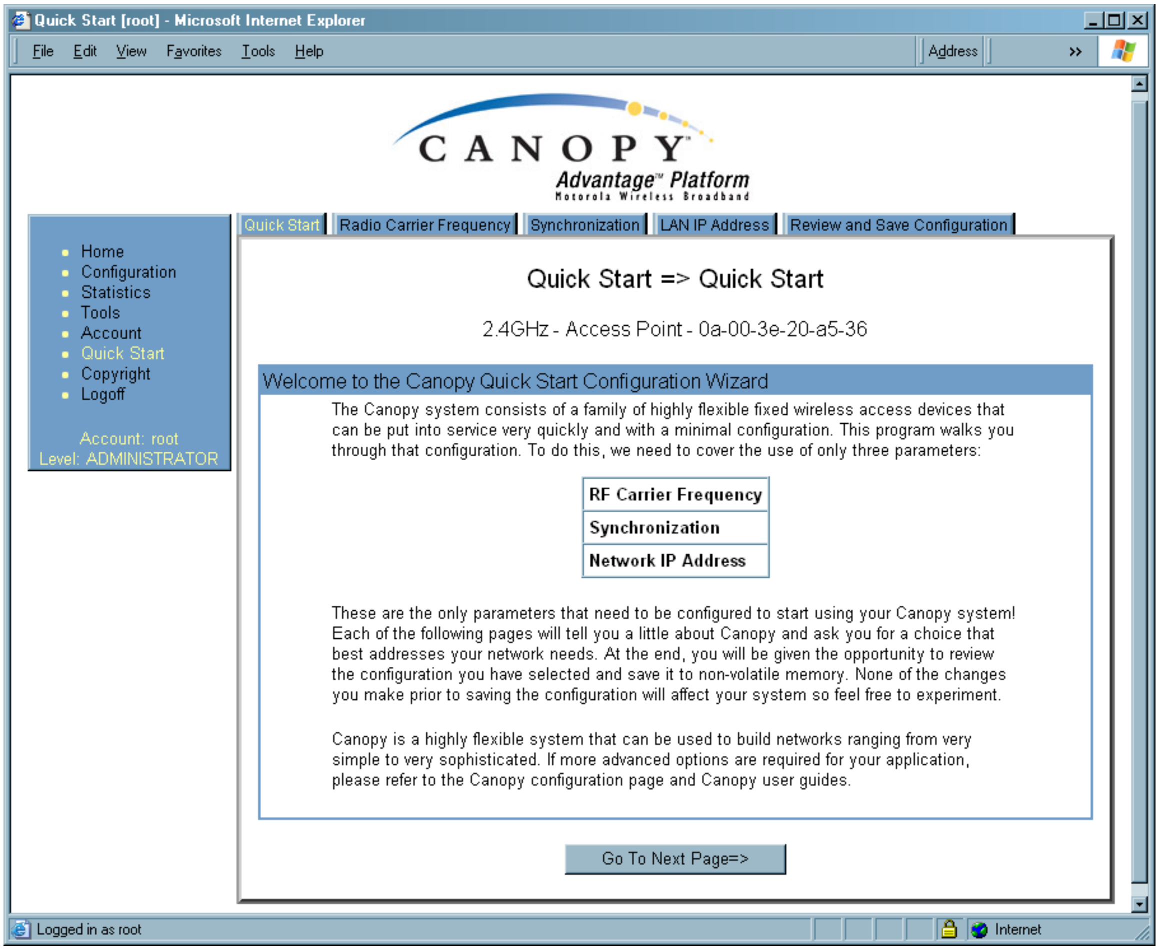
============================ **end of procedure** ============================

In the address bar of your browser, enter the IP address of the AP. (For example, enter **`http://169.254.1.1`** to access the AP through its default IP address). The AP responds by opening the General Status tab of its Home page.

16.3.1 Quick Start Page of the AP

To proceed with the test setup, click the **Quick Start** button on the left side of the General Status tab. The AP responds by opening the Quick Start page. The Quick Start tab of that page is displayed in Figure 52.

NOTE:
If you cannot find the IP address of the AP, see Override Plug on Page 58.



Quick Start => Quick Start

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

Welcome to the Canopy Quick Start Configuration Wizard

The Canopy system consists of a family of highly flexible fixed wireless access devices that can be put into service very quickly and with a minimal configuration. This program walks you through that configuration. To do this, we need to cover the use of only three parameters:

RF Carrier Frequency
Synchronization
Network IP Address

These are the only parameters that need to be configured to start using your Canopy system! Each of the following pages will tell you a little about Canopy and ask you for a choice that best addresses your network needs. At the end, you will be given the opportunity to review the configuration you have selected and save it to non-volatile memory. None of the changes you make prior to saving the configuration will affect your system so feel free to experiment.

Canopy is a highly flexible system that can be used to build networks ranging from very simple to very sophisticated. If more advanced options are required for your application, please refer to the Canopy configuration page and Canopy user guides.

Figure 52: Quick Start tab of AP, example

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

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

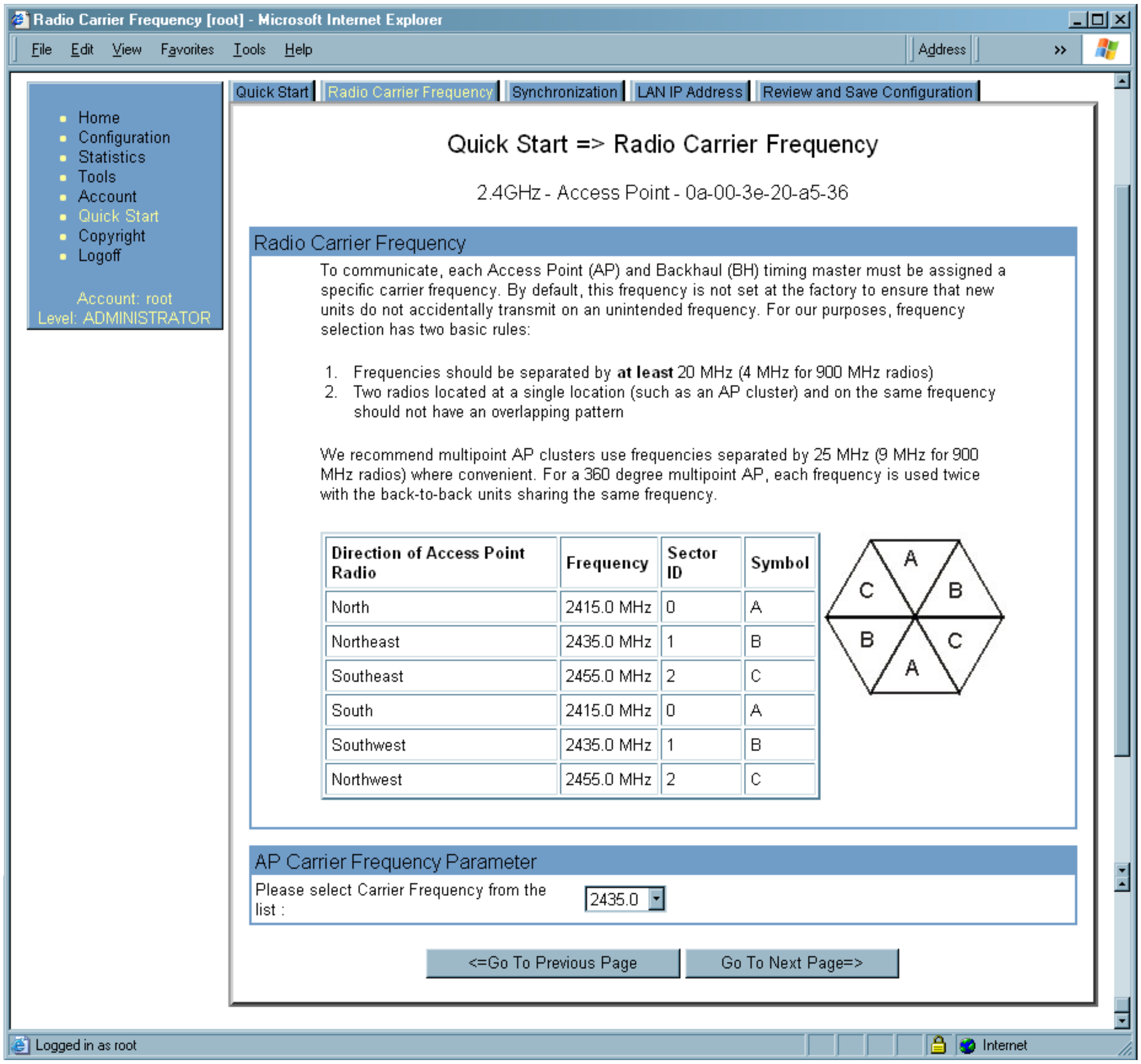
In each Quick Start tab, you can

- 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 7: Using Quick Start to configure a standalone AP for test

1. At the bottom of the Quick Start tab, click the **Go To Next Page =>** button.
   RESULT: The AP responds by opening the RF Carrier Frequency tab.
   An example of this tab is shown in Figure 53.



Quick Start => Radio Carrier Frequency

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

Radio Carrier Frequency

To communicate, each Access Point (AP) and Backhaul (BH) timing master must be assigned a specific carrier frequency. By default, this frequency is not set at the factory to ensure that new units do not accidentally transmit on an unintended frequency. For our purposes, frequency selection has two basic rules:

1. Frequencies should be separated by **at least** 20 MHz (4 MHz for 900 MHz radios)
2. Two radios located at a single location (such as an AP cluster) and on the same frequency should not have an overlapping pattern

We recommend multipoint AP clusters use frequencies separated by 25 MHz (9 MHz for 900 MHz radios) where convenient. For a 360 degree multipoint AP, each frequency is used twice with the back-to-back units sharing the same frequency.

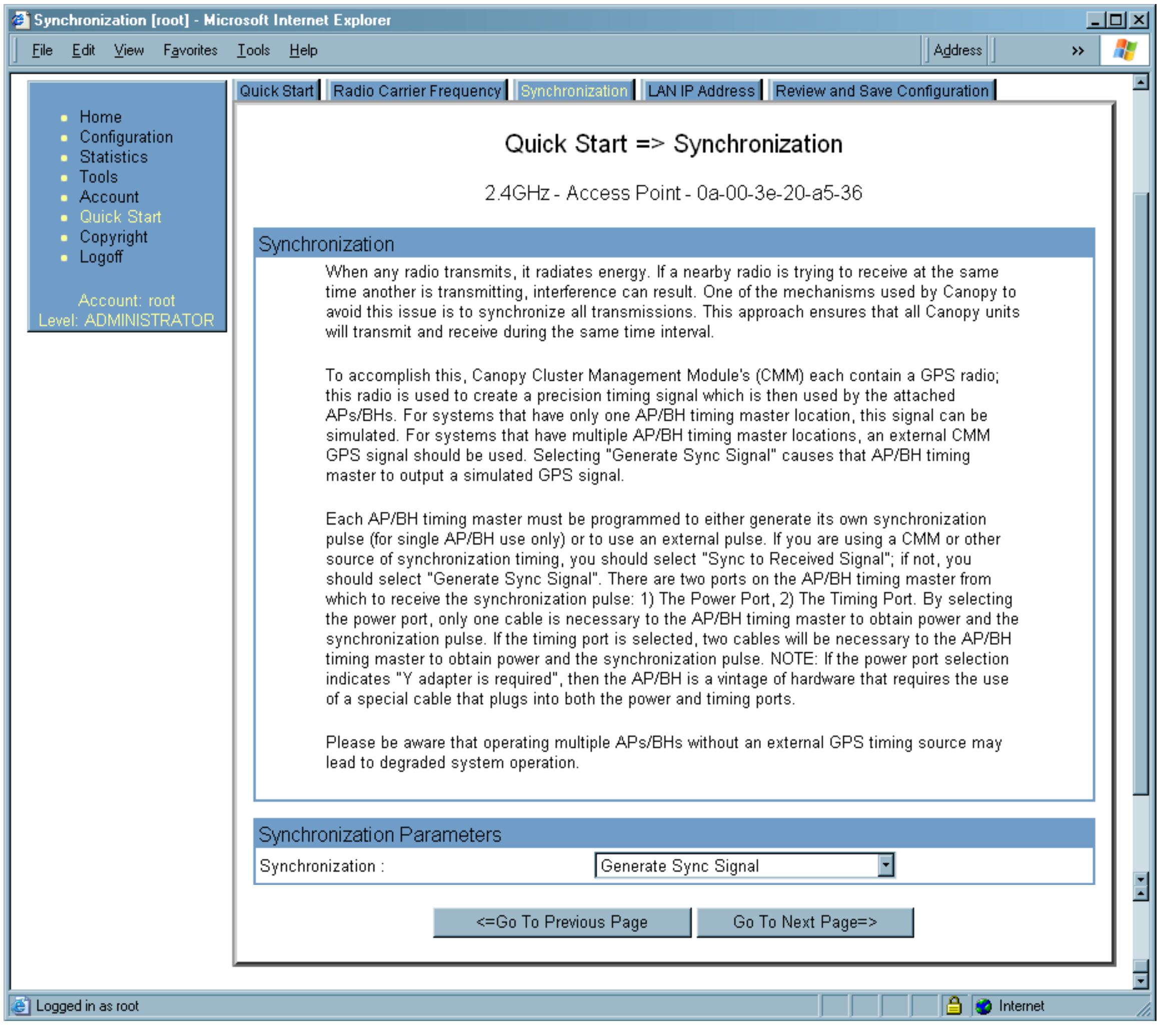
Direction of Access Point Radio	Frequency	Sector ID	Symbol
North	2415.0 MHz	0	A
Northeast	2435.0 MHz	1	B
Southeast	2455.0 MHz	2	C
South	2415.0 MHz	0	A
Southwest	2435.0 MHz	1	B
Northwest	2455.0 MHz	2	C

AP Carrier Frequency Parameter

Please select Carrier Frequency from the list : 2435.0

Figure 53: Radio Frequency Carrier tab of AP, example

2. From the pull-down menu in the lower left corner of this tab, select a frequency for the test.
3. Click the **Go To Next Page =>** button.
   RESULT: The AP responds by opening the Synchronization tab. An example of this tab is shown in Figure 54.



Account: root
Level: ADMINISTRATOR

Quick Start => Synchronization

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

Synchronization

When any radio transmits, it radiates energy. If a nearby radio is trying to receive at the same time another is transmitting, interference can result. One of the mechanisms used by Canopy to avoid this issue is to synchronize all transmissions. This approach ensures that all Canopy units will transmit and receive during the same time interval.

To accomplish this, Canopy Cluster Management Module's (CMM) each contain a GPS radio; this radio is used to create a precision timing signal which is then used by the attached APs/BHs. For systems that have only one AP/BH timing master location, this signal can be simulated. For systems that have multiple AP/BH timing master locations, an external CMM GPS signal should be used. Selecting "Generate Sync Signal" causes that AP/BH timing master to output a simulated GPS signal.

Each AP/BH timing master must be programmed to either generate its own synchronization pulse (for single AP/BH use only) or to use an external pulse. If you are using a CMM or other source of synchronization timing, you should select "Sync to Received Signal"; if not, you should select "Generate Sync Signal". There are two ports on the AP/BH timing master from which to receive the synchronization pulse: 1) The Power Port, 2) The Timing Port. By selecting the power port, only one cable is necessary to the AP/BH timing master to obtain power and the synchronization pulse. If the timing port is selected, two cables will be necessary to the AP/BH timing master to obtain power and the synchronization pulse. NOTE: If the power port selection indicates "Y adapter is required", then the AP/BH is a vintage of hardware that requires the use of a special cable that plugs into both the power and timing ports.

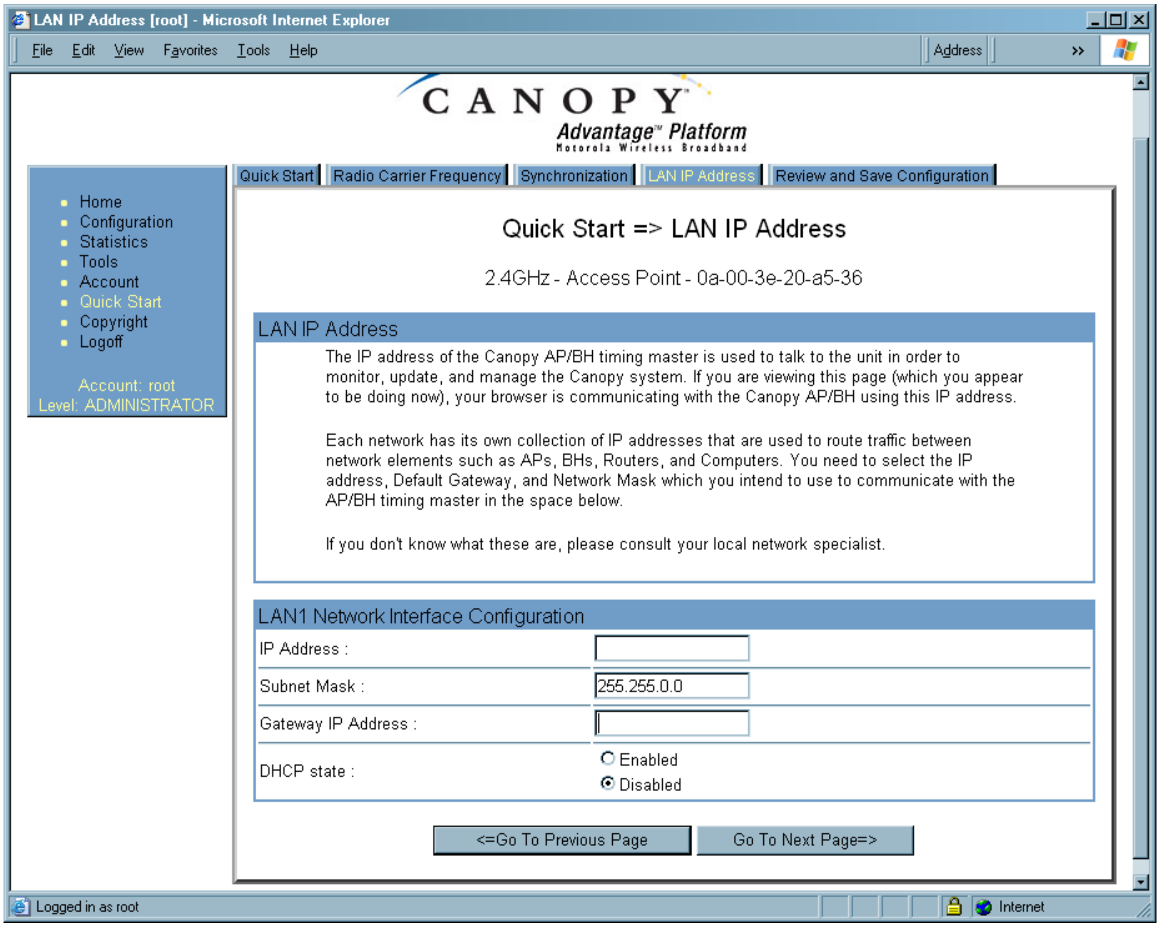
Please be aware that operating multiple APs/BHs without an external GPS timing source may lead to degraded system operation.

Synchronization Parameters

Synchronization : Generate Sync Signal

Figure 54: Synchronization tab of AP, example

4. At the bottom of this tab, select **Generate Sync Signal**.
5. Click the **Go To Next Page =>** button.
   RESULT: The AP responds by opening the LAN IP Address tab. An example of this tab is shown in Figure 55.



Quick Start => LAN IP Address

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

LAN IP Address

The IP address of the Canopy AP/BH timing master is used to talk to the unit in order to monitor, update, and manage the Canopy system. If you are viewing this page (which you appear to be doing now), your browser is communicating with the Canopy AP/BH using this IP address.

Each network has its own collection of IP addresses that are used to route traffic between network elements such as APs, BHs, Routers, and Computers. You need to select the IP address, Default Gateway, and Network Mask which you intend to use to communicate with the AP/BH timing master in the space below.

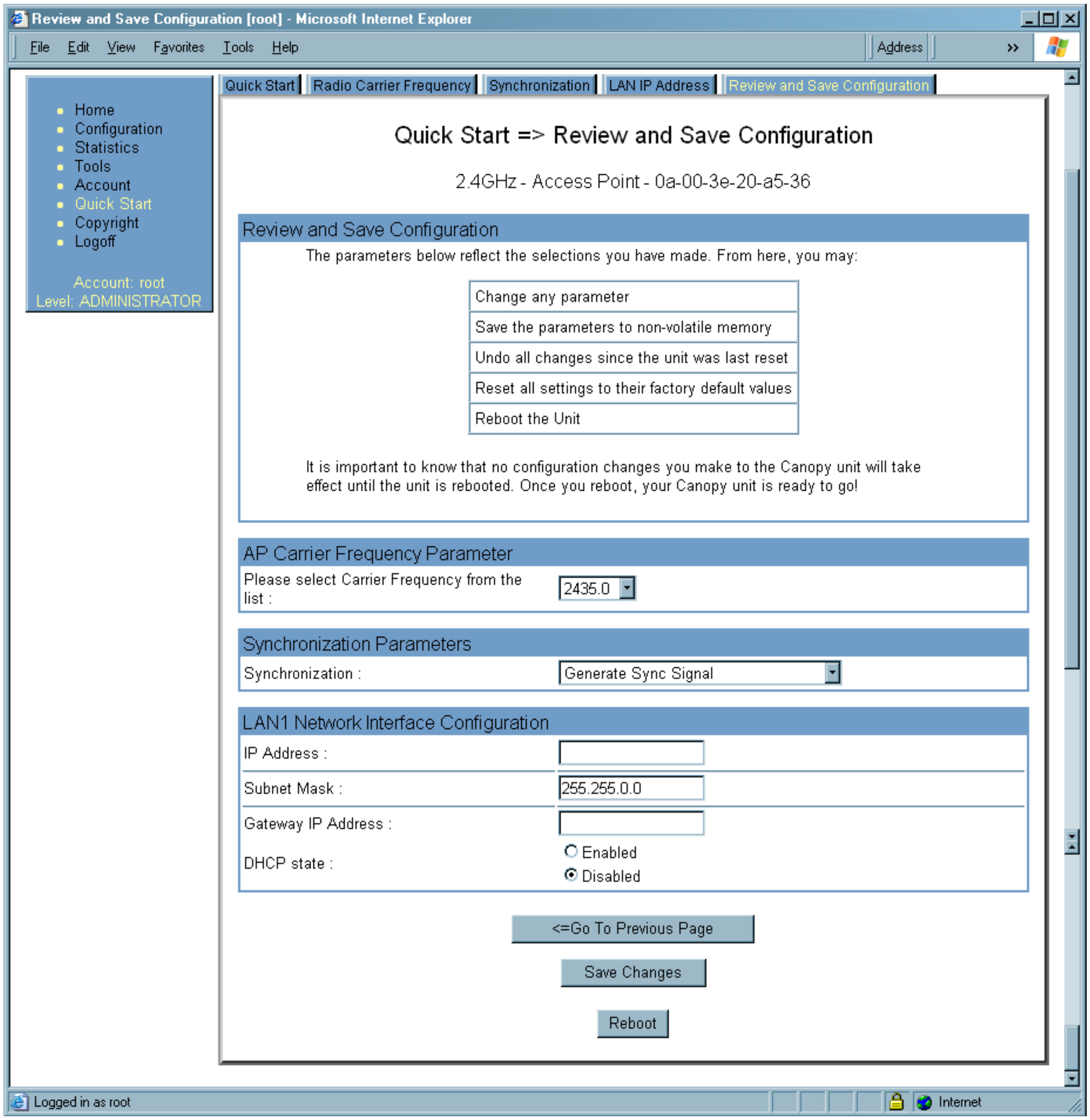
If you don't know what these are, please consult your local network specialist.

LAN1 Network Interface Configuration

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

Figure 55: LAN IP Address tab of AP, example

6. At the bottom of this tab, either
   - specify an **IP Address**, a **Subnet Mask**, and a **Gateway IP Address** for management of the AP 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 AP responds by opening the Review and Save Configuration tab. An example of this tab is shown in Figure 56.



Quick Start => Review and Save Configuration

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

Review and Save Configuration

The parameters below reflect the selections you have made. From here, you may:

- Change any parameter
- Save the parameters to non-volatile memory
- Undo all changes since the unit was last reset
- Reset all settings to their factory default values
- Reboot the Unit

It is important to know that no configuration changes you make to the Canopy unit will take effect until the unit is rebooted. Once you reboot, your Canopy unit is ready to go!

AP Carrier Frequency Parameter

Please select Carrier Frequency from the list :	2435.0

Synchronization Parameters

Synchronization :	Generate Sync Signal

LAN1 Network Interface Configuration

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

Figure 56: Review and Save Configuration tab of AP, example

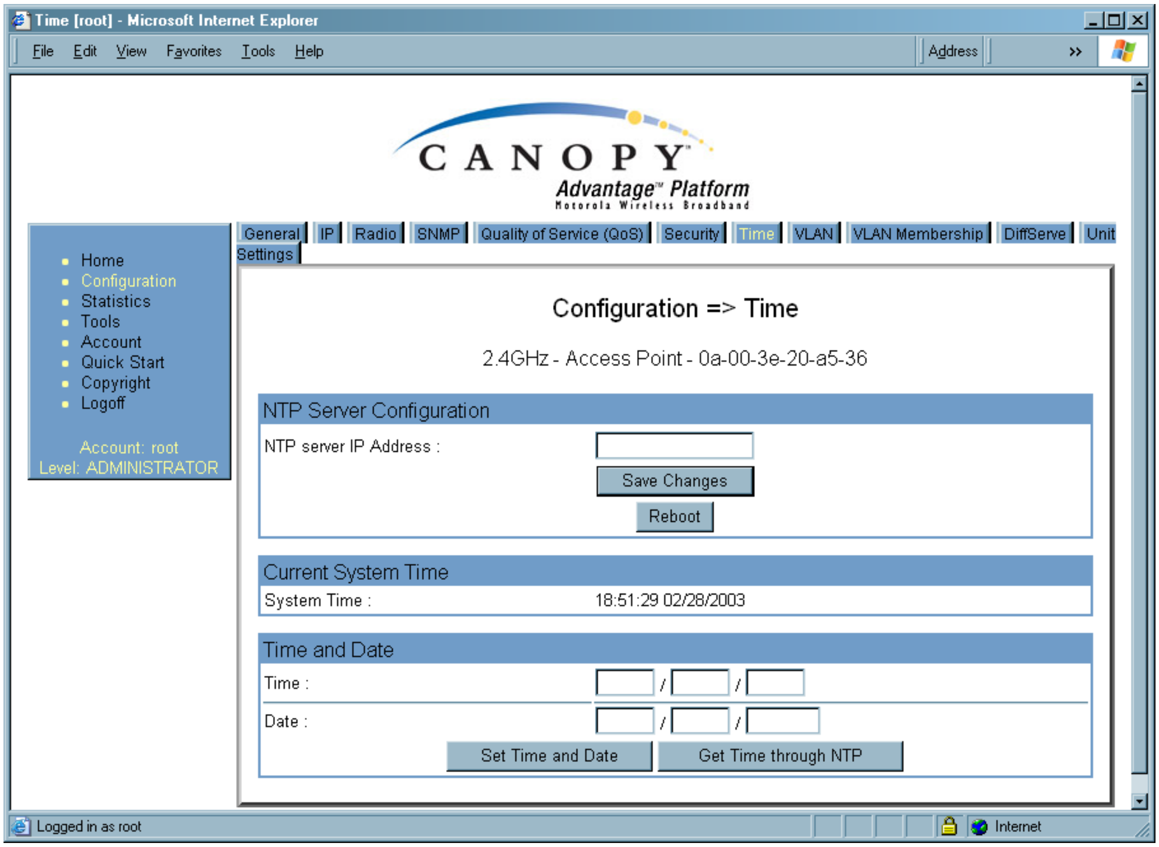
8. Ensure that the initial parameters for the AP are set as you intended.
9. Click the **Save Changes** button.
10. Click the **Reboot** button.
    RESULT: The AP responds with the message **Reboot Has Been Initiated…**
11. Wait until the indicator LEDs are not red.
12. Trigger your browser to refresh the page until the AP redisplays the General Status tab.
13. Wait until the red indicator LEDs are not lit.

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

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

16.3.2 Time Tab of the AP

To proceed with the test setup, click the **Configuration** link on the left side of the General Status tab. When the AP responds by opening the Configuration page to the General tab, click the Time tab. An example of this tab is displayed in Figure 57.



Configuration => Time

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

NTP Server Configuration

NTP server IP Address :

Current System Time

System Time : 18:51:29 02/28/2003

Time and Date

Time : / /

Date : / /

Figure 57: Time tab of AP, example

To have each log in the AP correlated to a meaningful time and date, either a reliable network element must pass time and date to the AP or you must set the time and date whenever a power cycle of the AP 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 both 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 AP.

If the AP should obtain 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 AP to obtain 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 :	***hh***	/	***mm***	/	***ss***
Date :	***MM***	/	***dd***	/	***yyyy***

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.

- Enter the appropriate information in the format shown above.
- Then 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.

Procedure 8: Setting up the SM for test

1. In one hand, securely hold the top (larger shell) of the SM. 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 SM RJ-45 jack.
3. Plug the other end of the Ethernet cable into the jack in the pig tail that hangs from the power supply.
4. Roughly aim the SM toward the AP.

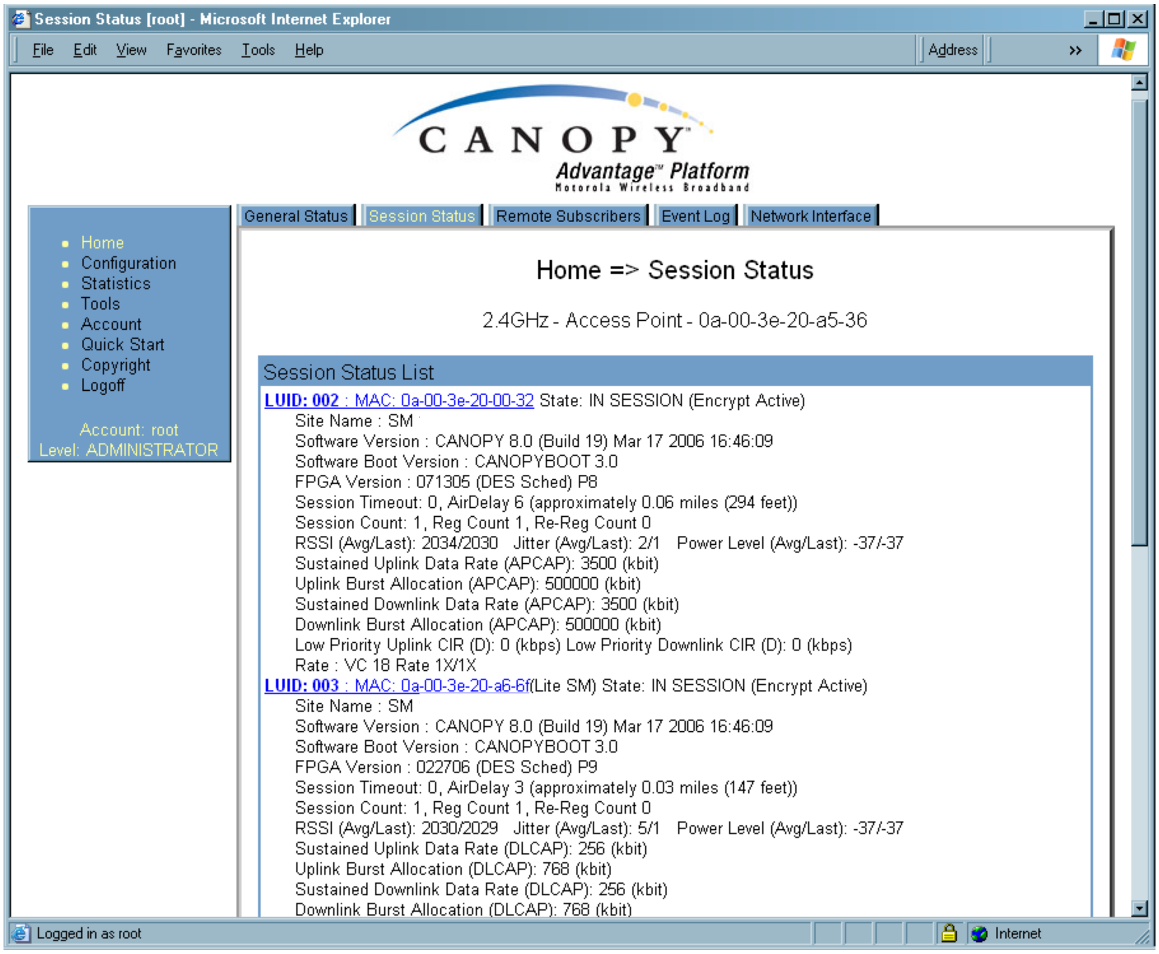
WARNING!
From this point until you remove power from the SM, stay at least as far from the SM as the minimum separation distance specified in Table 37 on Page 169.

5. Plug the power supply into an electrical outlet.
6. Repeat the foregoing steps for each SM that you wish to include in the test.
7. Back at the computing device, on the left side of the Time & Date tab, click **Home**.
8. Click the Session Status tab.

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

16.3.3 Session Status Tab of the AP

An example of the AP Session Status tab is displayed in Figure 58.



Home => Session Status

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

Session Status List

```
LUID: 002 : MAC: 0a-00-3e-20-00-32 State: IN SESSION (Encrypt Active)
    Site Name : SM
    Software Version : CANOPY 8.0 (Build 19) Mar 17 2006 16:46:09
    Software Boot Version : CANOPYBOOT 3.0
    FPGA Version : 071305 (DES Sched) P8
    Session Timeout: 0, AirDelay 6 (approximately 0.06 miles (294 feet))
    Session Count: 1, Reg Count 1, Re-Reg Count 0
    RSSI (Avg/Last): 2034/2030   Jitter (Avg/Last): 2/1   Power Level (Avg/Last): -37/-37
    Sustained Uplink Data Rate (APCAP): 3500 (kbit)
    Uplink Burst Allocation (APCAP): 500000 (kbit)
    Sustained Downlink Data Rate (APCAP): 3500 (kbit)
    Downlink Burst Allocation (APCAP): 500000 (kbit)
    Low Priority Uplink CIR (D): 0 (kbps) Low Priority Downlink CIR (D): 0 (kbps)
    Rate : VC 18 Rate 1X/1X
LUID: 003 : MAC: 0a-00-3e-20-a6-6f(Lite SM) State: IN SESSION (Encrypt Active)
    Site Name : SM
    Software Version : CANOPY 8.0 (Build 19) Mar 17 2006 16:46:09
    Software Boot Version : CANOPYBOOT 3.0
    FPGA Version : 022706 (DES Sched) P9
    Session Timeout: 0, AirDelay 3 (approximately 0.03 miles (147 feet))
    Session Count: 1, Reg Count 1, Re-Reg Count 0
    RSSI (Avg/Last): 2030/2029   Jitter (Avg/Last): 5/1   Power Level (Avg/Last): -37/-37
    Sustained Uplink Data Rate (DLCAP): 256 (kbit)
    Uplink Burst Allocation (DLCAP): 768 (kbit)
    Sustained Downlink Data Rate (DLCAP): 256 (kbit)
    Downlink Burst Allocation (DLCAP): 768 (kbit)
```

Figure 58: Session Status tab data from AP, example

If no SMs are registered to this AP, then the Session Status tab displays the simple message **No sessions**. In this case, try the following steps.

Procedure 9: Retrying to establish a point-to-multipoint link

1. More finely aim the SM or SMs toward the AP.
2. Recheck the Session Status tab of the AP for the presence of LUIDs.
3. If still no LUIDs are reported on the Session Status tab, click the **Configuration** button on the left side of the Home page.
   RESULT: The AP responds by opening the AP Configuration page.
4. Click the Radio tab.
5. Find the **Color Code** parameter and note the setting.
6. In the same sequence as you did for the AP directly under Configuring a Point-to-Multipoint Link for Test on Page 184, connect the SM to a computing device and to power.

7. On the left side of the SM Home page, click the **Configuration** button.
   RESULT: The Configuration page of the SM opens.
8. Click the Radio tab.
9. If the transmit frequency of the AP is not selected in the **Custom Radio Frequency Scan Selection List** parameter, select the frequency that matches.
10. If the **Color Code** parameter on this page is not identical to the **Color Code** parameter you noted from the AP, change one of them so that they match.
11. At the bottom of the Radio tab for the SM, click the **Save Changes** button.
12. Click the **Reboot** button.
13. Allow several minutes for the SM to reboot and register to the AP.
14. Return to the computing device that is connected to the AP.
15. Recheck the Session Status tab of the AP for the presence of LUIDs.

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

The Session Status tab provides information about each SM that has registered to the AP. This information is useful for managing and troubleshooting a Cyclone system. All information that you have entered in the **Site Name** field of the SM displays in the Session Status tab of the linked AP.

The Session Status tab also includes the current active values on each SM (LUID) for MIR, CIR, and VLAN, as well as the source of these values (representing the SM itself, BAM, or the AP and cap, if any—for example, APCAP as shown in Figure 58 above). L indicates a Cyclone Lite SM, and D indicates from the device. As an SM registers to the AP, the configuration source that this page displays for the associated LUID may change. After registration, however, the displayed source is stable and can be trusted.

The Session Status tab of the AP provides the following parameters.

LUID

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

> *NOTE:*
> The LUID association is lost when a power cycle of the AP occurs.

MAC

This field displays the MAC address (or electronic serial number) of the SM.

State

This field displays the current status of the SM as either

- **IN SESSION** to indicate that the SM is currently registered to the AP.
- **IDLE** to indicate that the SM was registered to the AP at one time, but now is not.

This field also indicates whether the encryption scheme in the module is enabled.

Site Name

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

Software Version

This field displays the software release that operates on the SM, the release date and time of the software.

Software Boot Version

This field indicates the CYCLONEBOOT version number.

FPGA Version

This field displays the version of FPGA that runs on the SM.

Session Timeout

This field displays the timeout in seconds for management sessions via HTTP, telnet, or ftp access to the SM. 0 indicates that no limit is imposed.

AirDelay

This field displays the distance of the SM from the AP. To derive the distance in meters, multiply the displayed number by 0.3048. At close distances, the value in this field is unreliable.

Session Count

This field displays how many sessions the SM has had with the AP. Typically, this is the sum of Reg Count and Re-Reg Count. However, the result of internal calculation may display here as a value that slightly differs from the sum.

If the number of sessions is significantly greater than the number for other SMs, then this may indicate a link problem or an interference problem.

Reg Count

When an SM makes a registration request, the AP checks its local data to see whether it considers the SM to be already registered. If the AP concludes that the SM is not, then the request increments the value of this field.

Re-Reg Count

When an SM makes a registration request, the AP checks its local data to see whether it considers the SM to be already registered. If the AP concludes that the SM is not, then the request increments the value of this field. Typically, a Re-Reg is the case where both

- an SM attempts to reregister for having lost communication with the AP.
- the AP has not yet observed the link to the SM as being down.

A high number in this field is often an indication of link instability or interference problems.

RSSI, Jitter, and Power Level (Avg/Last)

The Session 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 an SM a power level of −75 dBm and a jitter measurement of 5, and further refining the alignment drops the power level to −78 dBm and the jitter to 2 or 3, 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.

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

Sustained Uplink Data Rate

This field displays the value that is currently in effect for the SM, with the source of that value in parentheses. This is the specified rate at which each SM registered to this AP is replenished with credits for transmission. The configuration source of the value is indicated in parentheses. 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 295.

Uplink Burst Allocation

This field displays the value that is currently in effect for the SM, with the source of that value in parentheses. This is the specified maximum amount of data that each SM is allowed to transmit before being recharged at the **Sustained Uplink Data Rate** with credits to transmit more. The configuration source of the value is indicated in parentheses. 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 295.

Sustained Downlink Data Rate

This field displays the value that is currently in effect for the SM, with the source of that value in parentheses. This is the specified the rate at which the AP should be replenished with credits (tokens) for transmission to each of the SMs in its sector. The configuration source of the value is indicated in parentheses. 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 295.

Downlink Burst Allocation

This field displays the value that is currently in effect for the SM, with the source of that value in parentheses. This is 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**. The configuration source of the value is indicated in parentheses. 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 295.

Low Priority Uplink CIR

This field displays the value that is currently in effect for the SM, with the source of that value in parentheses. The configuration source of the value is indicated in parentheses. See

- Committed Information Rate on Page 86
- Setting the Configuration Source on Page 295.

Low Priority Downlink CIR

This field displays the value that is currently in effect for the SM, with the source of that value in parentheses. The configuration source of the value is indicated in parentheses. See

- Committed Information Rate on Page 86
- Setting the Configuration Source on Page 295.

Rate

This field displays whether the high-priority channel is enabled in the SM and the status of 1X or 2X operation in the SM. See Checking the Status of 2X Operation on Page 92.

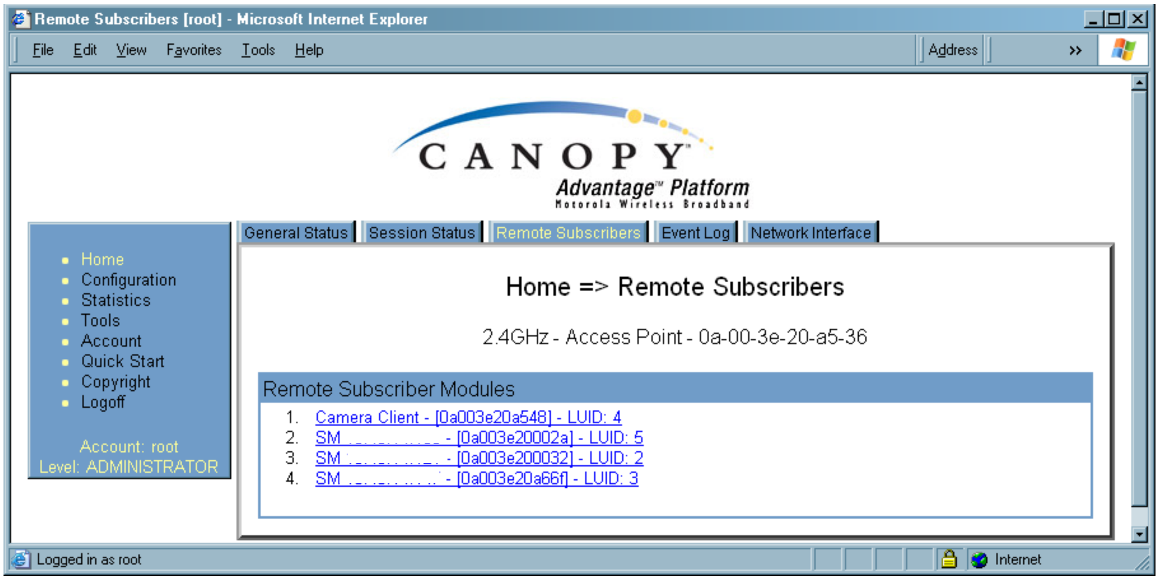
16.3.4 Beginning the Test of Point-to-Multipoint Links

To begin the test of links, perform the following steps:

1. In the Session Status tab of the AP, note the LUID associated with the MAC address of any SM you wish to involve in the test.
2. Click the Remote Subscribers tab.

16.3.5 Remote Subscribers Tab of the AP

An example of a Remote Subscribers tab is displayed in Figure 59.



Account: root
Level: ADMINISTRATOR

Home => Remote Subscribers

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

Remote Subscriber Modules

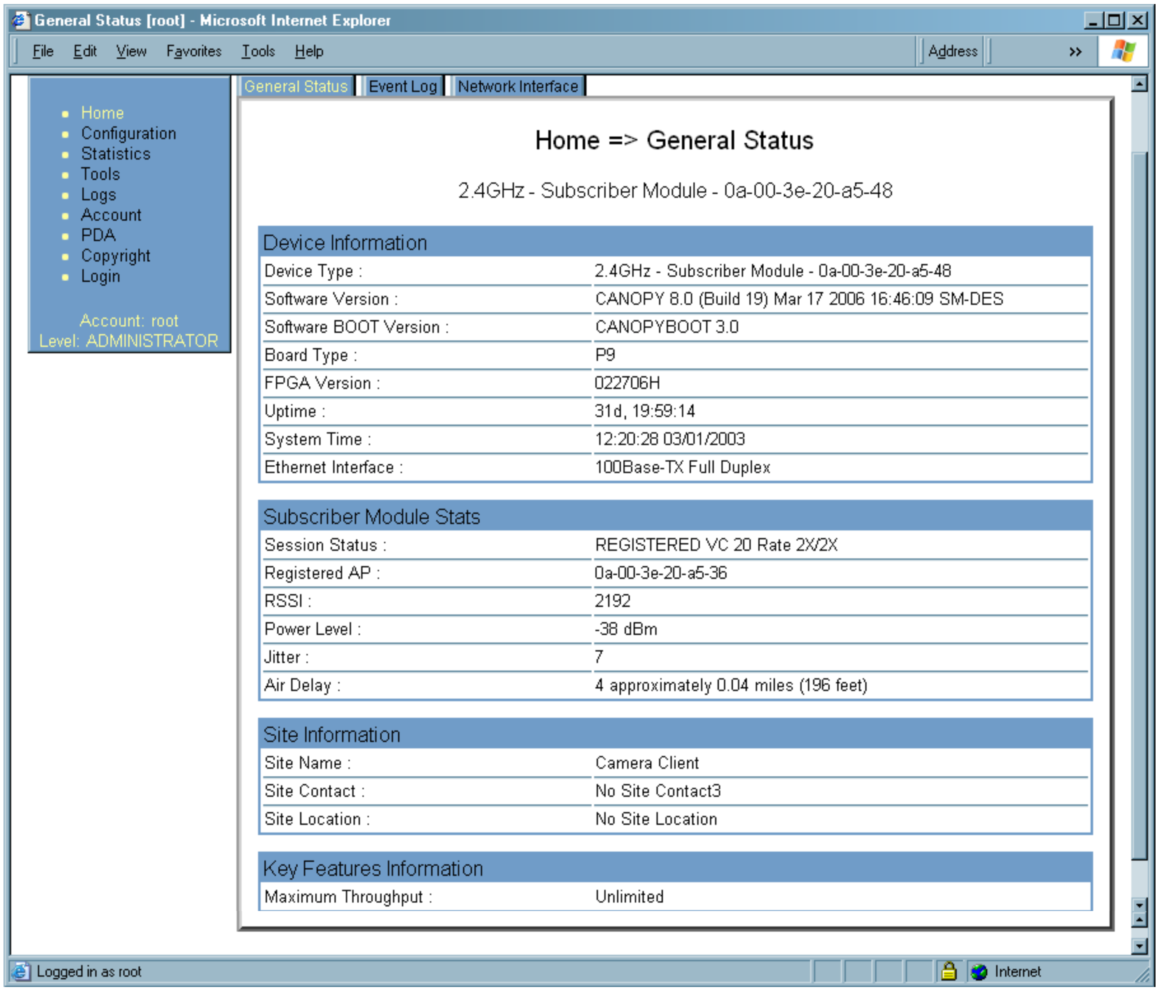
1. Camera Client - [0a003e20a548] - LUID: 4
2. SM [illegible] - [0a003e20002a] - LUID: 5
3. SM [illegible] - [0a003e200032] - LUID: 2
4. SM [illegible] - [0a003e20a66f] - LUID: 3

Figure 59: Remote Subscribers tab of AP, example

This tab allows you to view the web pages of registered SMs over the RF link. To view the pages for a selected SM, click its link. The General Status tab of the SM opens.

16.3.6 General Status Tab of the SM

An example of the General Status tab of an SM is displayed in Figure 60.



Home => General Status

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

Device Information	
Device Type :	2.4GHz - Subscriber Module - 0a-00-3e-20-a5-48
Software Version :	CANOPY 8.0 (Build 19) Mar 17 2006 16:46:09 SM-DES
Software BOOT Version :	CANOPYBOOT 3.0
Board Type :	P9
FPGA Version :	022706H
Uptime :	31d, 19:59:14
System Time :	12:20:28 03/01/2003
Ethernet Interface :	100Base-TX Full Duplex

Subscriber Module Stats	
Session Status :	REGISTERED VC 20 Rate 2X/2X
Registered AP :	0a-00-3e-20-a5-36
RSSI :	2192
Power Level :	-38 dBm
Jitter :	7
Air Delay :	4 approximately 0.04 miles (196 feet)

Site Information	
Site Name :	Camera Client
Site Contact :	No Site Contact3
Site Location :	No Site Location

Key Features Information	
Maximum Throughput :	Unlimited

Figure 60: General Status tab of SM, example

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

Device Type

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

Software Version

This field indicates the Cyclone system release, the time and date of the release, and whether communications involving the module are secured by DES or AES encryption (see Encrypting Cyclone Radio Transmissions on Page 375). If you request technical support, provide the information from this field.

Software BOOT Version

This field indicates the version of the CYCLONEBOOT 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 372.

FPGA Version

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

Uptime

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

System Time

This field provides the current time. Any SM that registers to an AP inherits the system time, which is displayed in this field as GMT (Greenwich Mean Time).

Ethernet Interface

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

Session Status

This field displays the following information about the current session:

- **Scanning** indicates that this SM currently cycles through the radio frequencies that are selected in the Radio tab of the Configuration page.
- **Syncing** indicates that this SM currently attempts to receive sync.
- **Registering** indicates that this SM has sent a registration request message to the AP and has not yet received a response.
- **Registered** indicates that this SM is both
  - 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 AP to which this SM 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 an SM a power level of −75 dBm and a jitter measurement of 5, and further refining the alignment drops the power level to −78 dBm and the jitter to 2 or 3, 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 this SM and the AP. To derive the distance in meters, multiply the value of this parameter by 0.3048. Distances reported as less than 200 feet (61 meters) are unreliable.

Site Name

This field indicates the name of the physical module. You can assign or change this name in the SNMP tab of the SM Configuration page. This information is also set into the *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 SM 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 SM Configuration page.

Maximum Throughput

This field indicates the limit of aggregate throughput for the SM and is based on the default (factory) limit of the SM and any floating license that is currently assigned to it.

16.3.7 Continuing the Test of Point-to-Multipoint Links

To resume the test of links, perform the following steps.

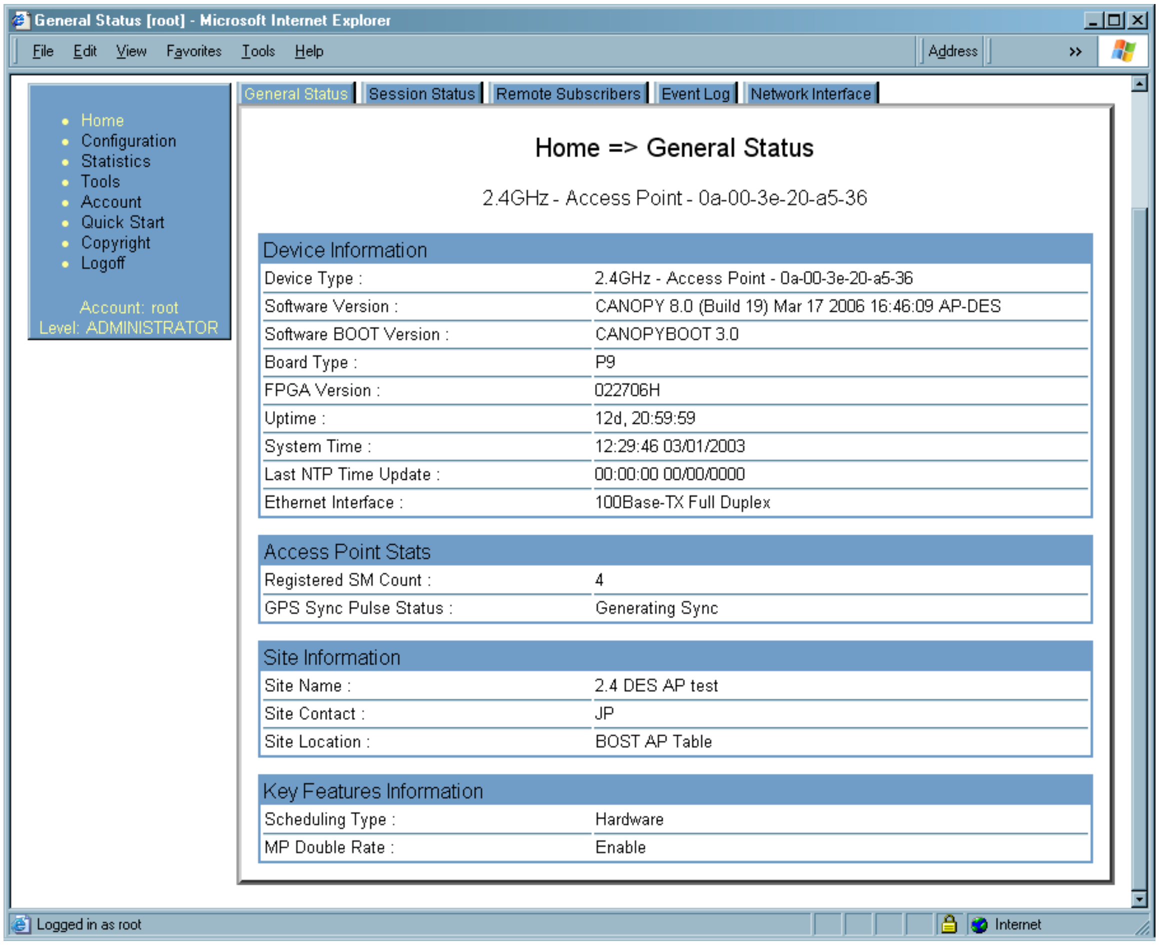
Procedure 10: Verifying and recording information from SMs

1. Verify that the **Session Status** field of the General Status tab in the SM indicates **REGISTERED**.
2. While you view the General Status tab in the SM, 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 (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.



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 :	022706H
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

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 Cyclone module. Values include the frequency band of the AP, its module type, and its MAC address.

Software Version

This field indicates the Cyclone system release, the time and date of the release, and whether communications involving the module are secured by DES or AES encryption (see Encrypting Cyclone Radio Transmissions on Page 375). If you request technical support, provide the information from this field.

Software BOOT Version

This field indicates the version of the CYCLONEBOOT 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 372.

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

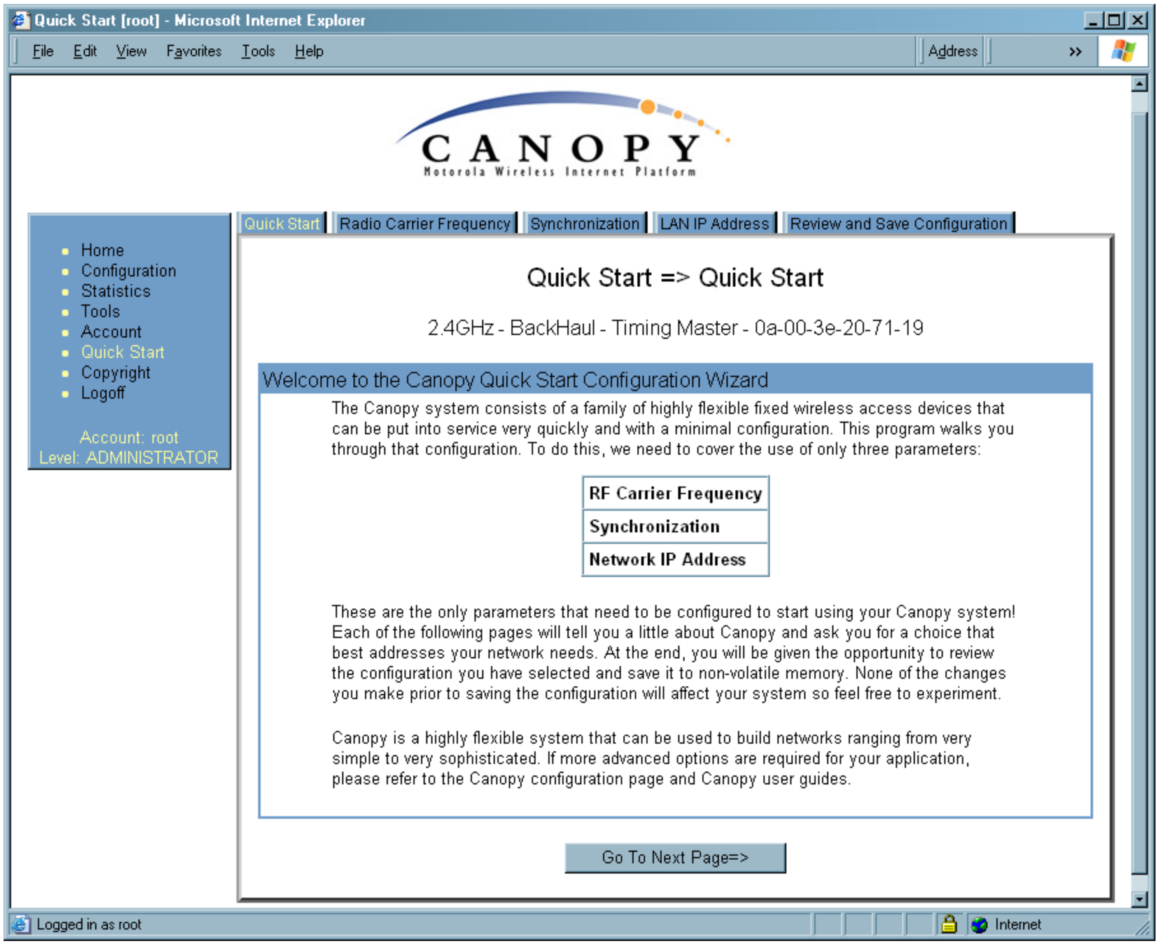
You can access the web-based interface through only a computing device that is either directly connected or connected through a network to the BH. If the computing device is not connected to a network when you are configuring the module in your test environment, and if the computer has used a proxy server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



Quick Start => Quick Start

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

Welcome to the Canopy Quick Start Configuration Wizard

The Canopy system consists of a family of highly flexible fixed wireless access devices that can be put into service very quickly and with a minimal configuration. This program walks you through that configuration. To do this, we need to cover the use of only three parameters:

RF Carrier Frequency
Synchronization
Network IP Address

These are the only parameters that need to be configured to start using your Canopy system! Each of the following pages will tell you a little about Canopy and ask you for a choice that best addresses your network needs. At the end, you will be given the opportunity to review the configuration you have selected and save it to non-volatile memory. None of the changes you make prior to saving the configuration will affect your system so feel free to experiment.

Canopy is a highly flexible system that can be used to build networks ranging from very simple to very sophisticated. If more advanced options are required for your application, please refer to the Canopy configuration page and Canopy user guides.

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

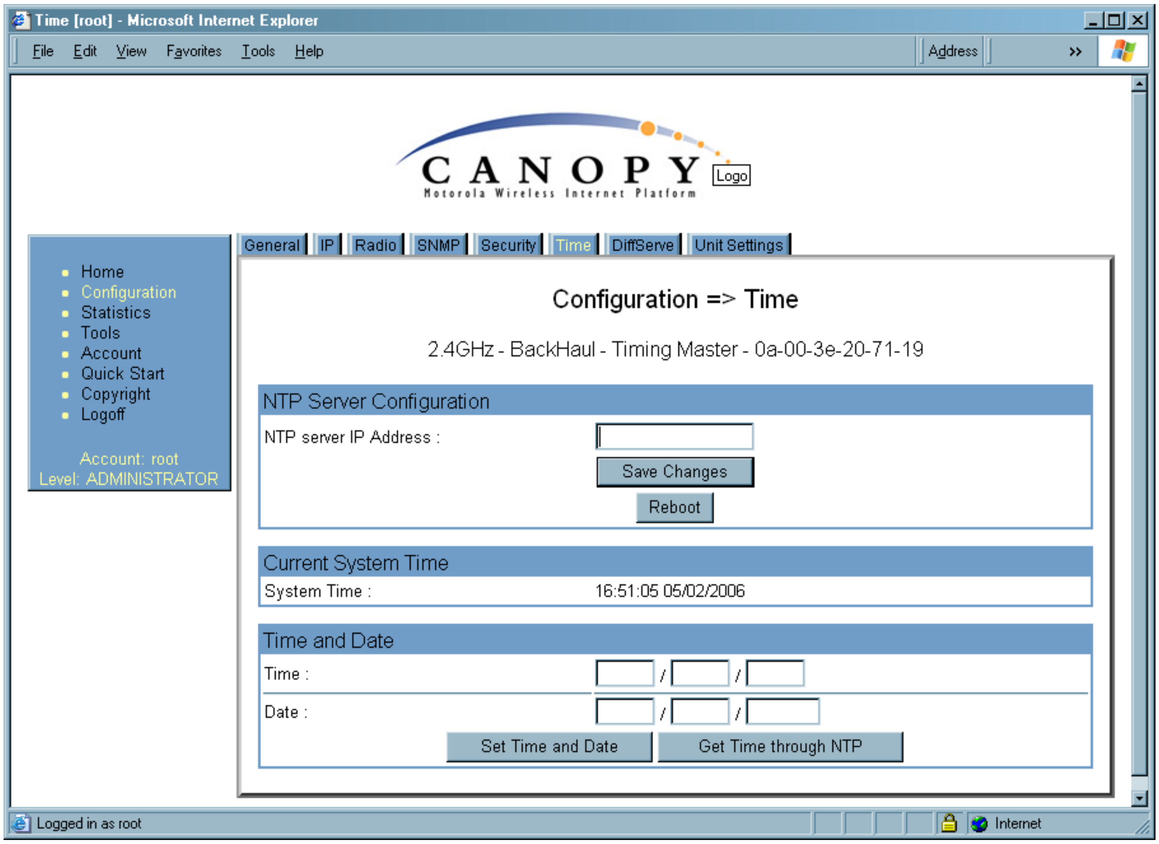
1. At the bottom of the Quick Start tab, click the **Go To Next Page =>** button.
   RESULT: The BHM responds by opening the RF Carrier Frequency tab.
2. From the pull-down menu in the lower left corner of this page, select a frequency for the test.
3. Click the **Go To Next Page =>** button.
   RESULT: 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 redisplays 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** ===========================

Cyclone 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.



Account: root
Level: ADMINISTRATOR

Configuration => Time

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

NTP Server Configuration

NTP server IP Address :

Current System Time

System Time : 16:51:05 05/02/2006

Time and Date

Time : / /

Date : / /

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 :	***hh***	/	***mm***	/	***ss***
Date :	***MM***	/	***dd***	/	***yyyy***

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.

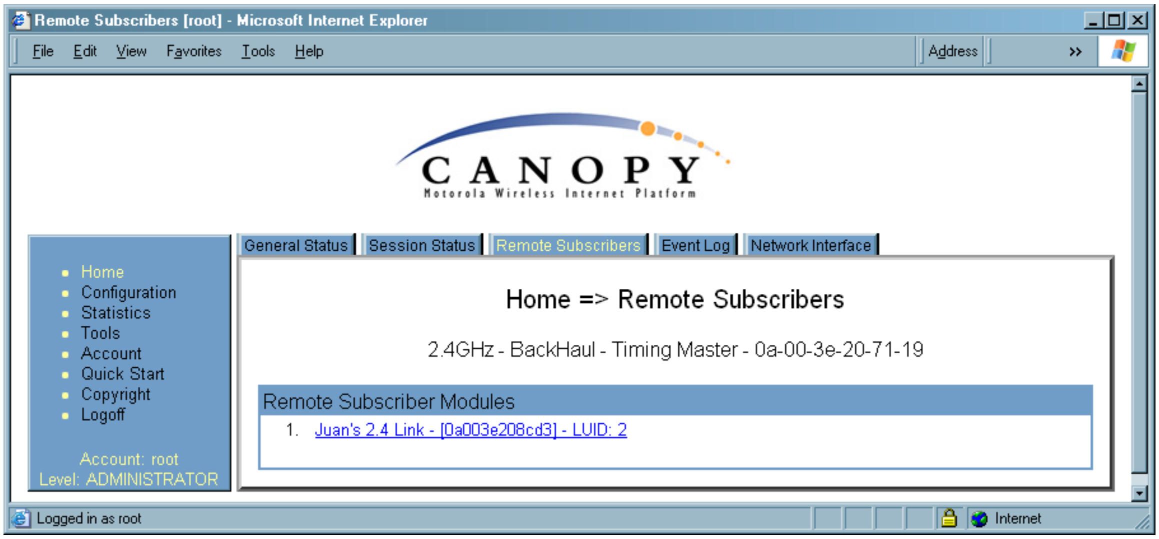
Procedure 14: Setting up the BHS for test

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** ================================



Home => Remote Subscribers

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

Remote Subscriber Modules

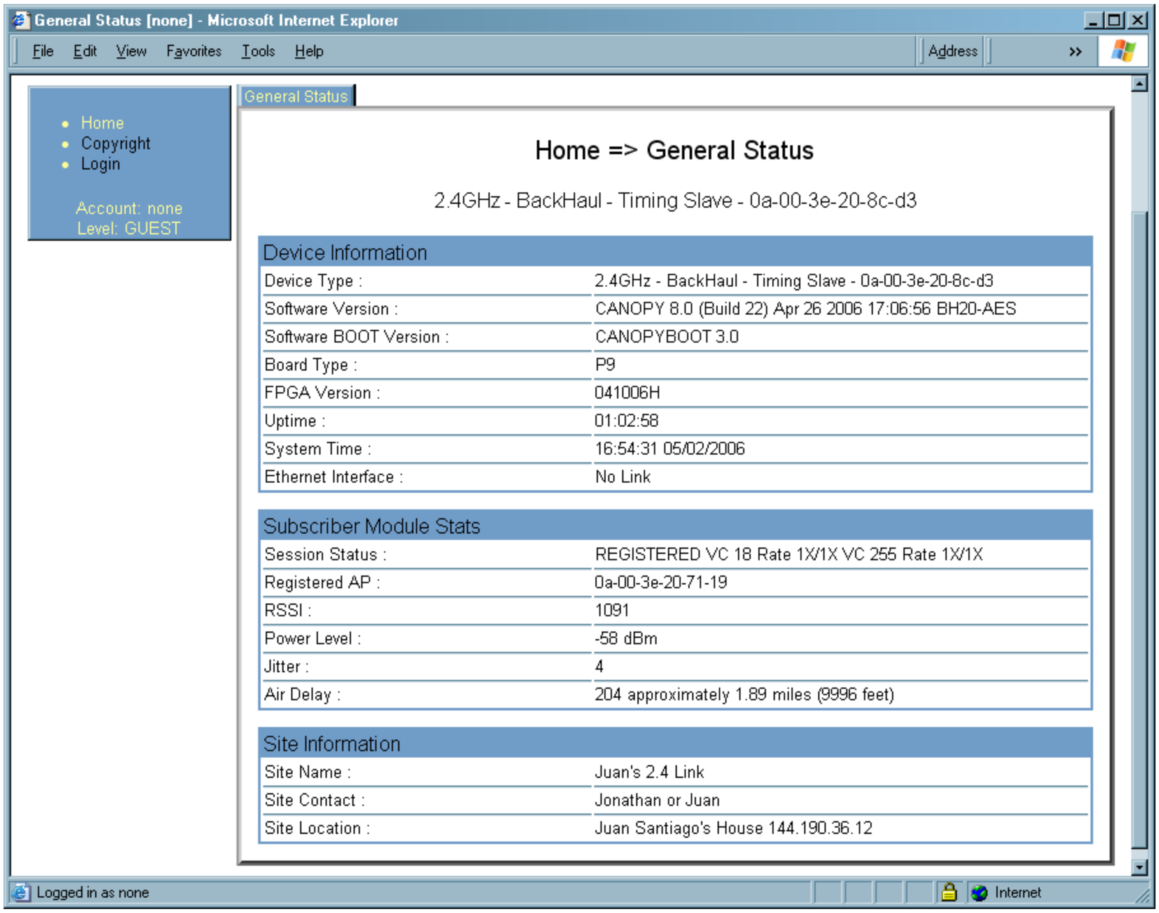
1. Juan's 2.4 Link - [0a003e208cd3] - LUID: 2

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.



Home => General Status

2.4GHz - BackHaul - Timing Slave - 0a-00-3e-20-8c-d3

Device Information	
Device Type :	2.4GHz - BackHaul - Timing Slave - 0a-00-3e-20-8c-d3
Software Version :	CANOPY 8.0 (Build 22) Apr 26 2006 17:06:56 BH20-AES
Software BOOT Version :	CANOPYBOOT 3.0
Board Type :	P9
FPGA Version :	041006H
Uptime :	01:02:58
System Time :	16:54:31 05/02/2006
Ethernet Interface :	No Link

Subscriber Module Stats	
Session Status :	REGISTERED VC 18 Rate 1X/1X VC 255 Rate 1X/1X
Registered AP :	0a-00-3e-20-71-19
RSSI :	1091
Power Level :	-58 dBm
Jitter :	4
Air Delay :	204 approximately 1.89 miles (9996 feet)

Site Information	
Site Name :	Juan's 2.4 Link
Site Contact :	Jonathan or Juan
Site Location :	Juan Santiago's House 144.190.36.12

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 Cyclone module. Values include the frequency band of the BHS, its module type, and its MAC address.

Software Version

This field indicates the Cyclone 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 Cyclone Radio Transmissions on Page 375). If you request technical support, provide the information from this field.

Software BOOT Version

This field indicates the version of the CYCLONEBOOT 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 372.

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

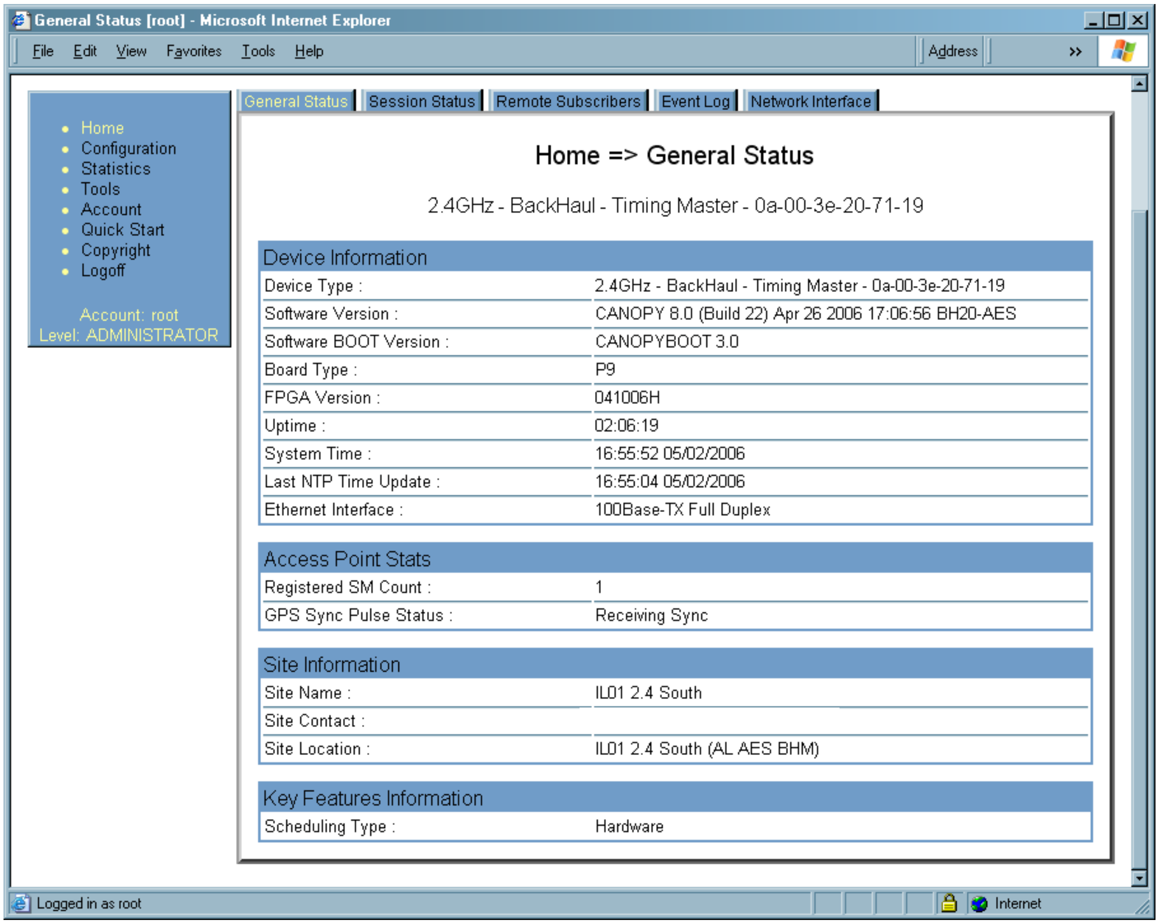
1. Verify that the **Session Status** field of the General Status tab in the BHS indicates **REGISTERED**.
   NOTE: This indication confirms that the BHS is properly functional.
2. While your browser is set to the General Status tab, note (or print) the values of the following fields:
   - **Device type**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



Home => General Status

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

Device Information	
Device Type :	2.4GHz - BackHaul - Timing Master - 0a-00-3e-20-71-19
Software Version :	CANOPY 8.0 (Build 22) Apr 26 2006 17:06:56 BH20-AES
Software BOOT Version :	CANOPYBOOT 3.0
Board Type :	P9
FPGA Version :	041006H
Uptime :	02:06:19
System Time :	16:55:52 05/02/2006
Last NTP Time Update :	16:55:04 05/02/2006
Ethernet Interface :	100Base-TX Full Duplex

Access Point Stats	
Registered SM Count :	1
GPS Sync Pulse Status :	Receiving Sync

Site Information	
Site Name :	IL01 2.4 South
Site Contact :	
Site Location :	IL01 2.4 South (AL AES BHM)

Key Features Information	
Scheduling Type :	Hardware

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 Cyclone 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 Cyclone Radio Transmissions on Page 375). When you request technical support, provide the information from this field.

Software BOOT Version

This field indicates the version of the CYCLONEBOOT 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 372.

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 Cyclone 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

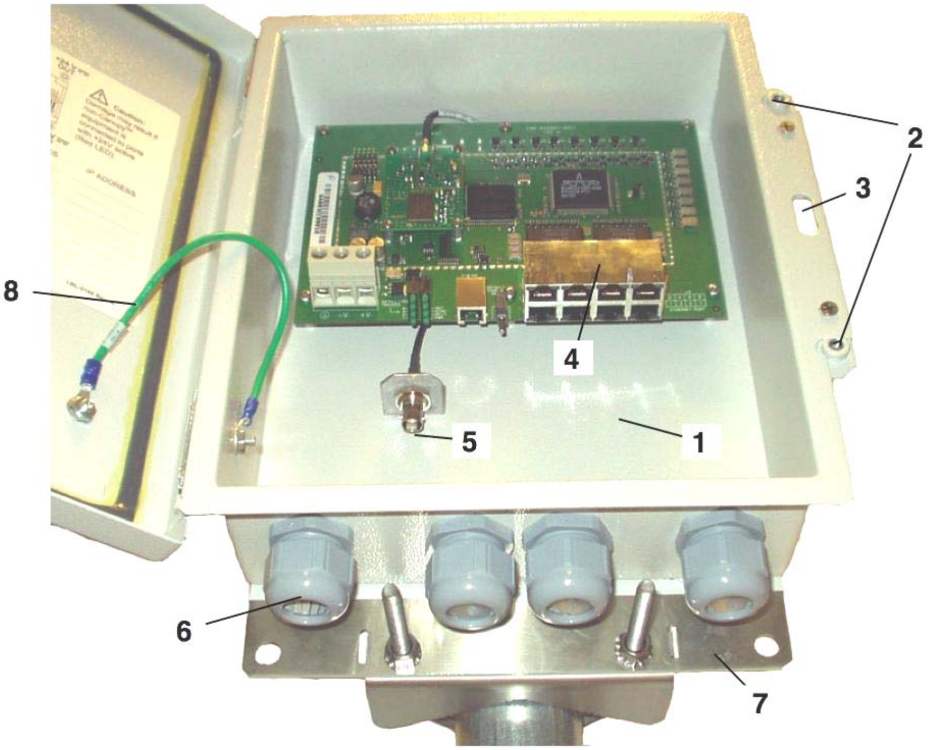
1. Confirm that the **GPS Sync Pulse Status** field indicates **Generating Sync**.
   NOTE: This indication confirms that the BHM is properly functional.
2. While your browser is set to this BHM Status page, note (or print) the values of the following fields:
   - **Device type**
   - **Software Version**
   - **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.

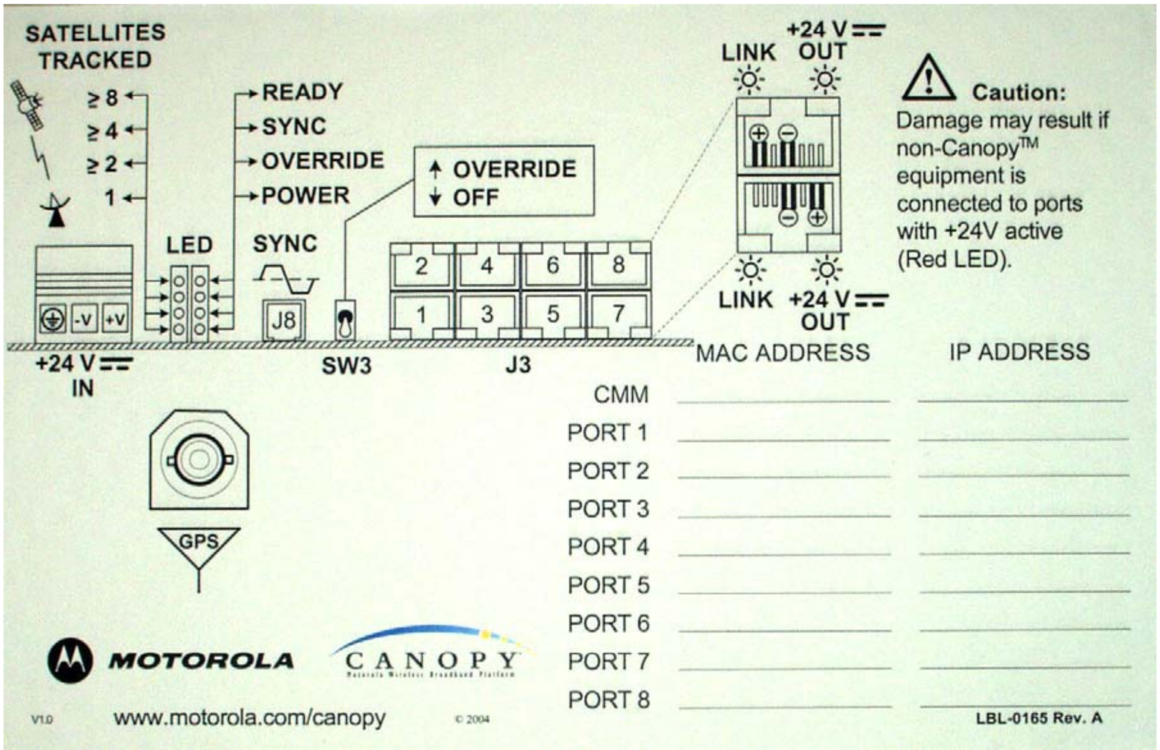
Procedure 17: Setting up a CMMmicro

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 219.

CAUTION!
Never connect any devices other than Cyclone 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 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 70 on Page 221.
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.

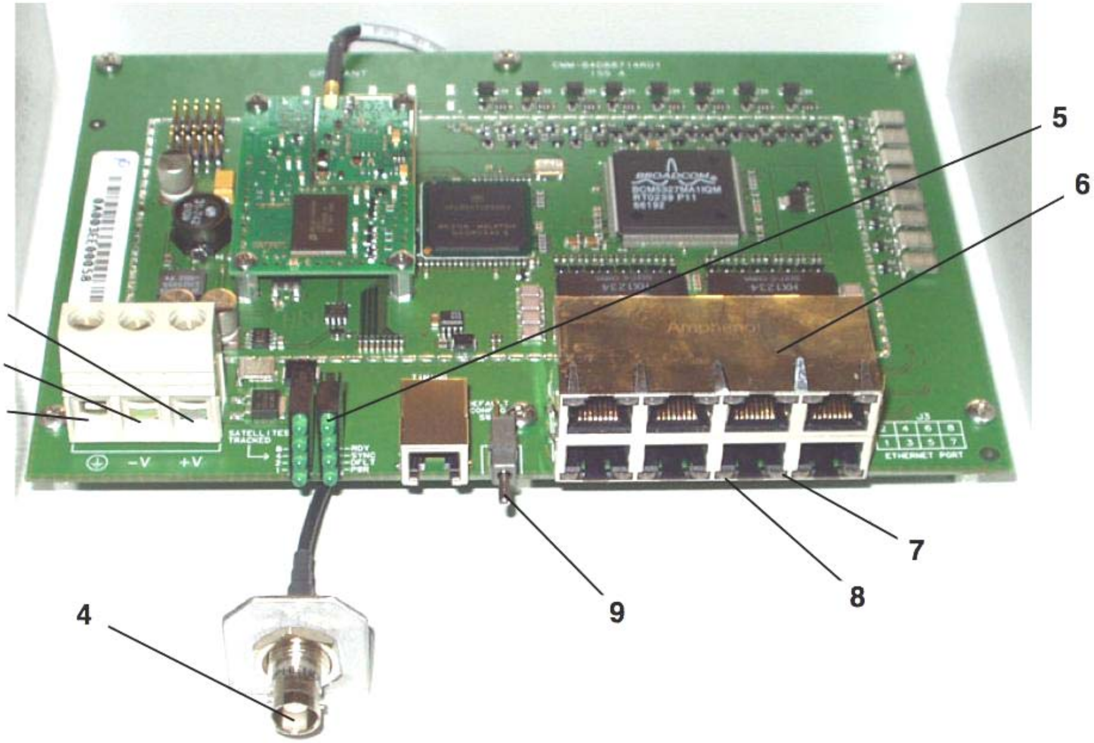
========================= **end of procedure** =========================



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 68: CMMmicro door label

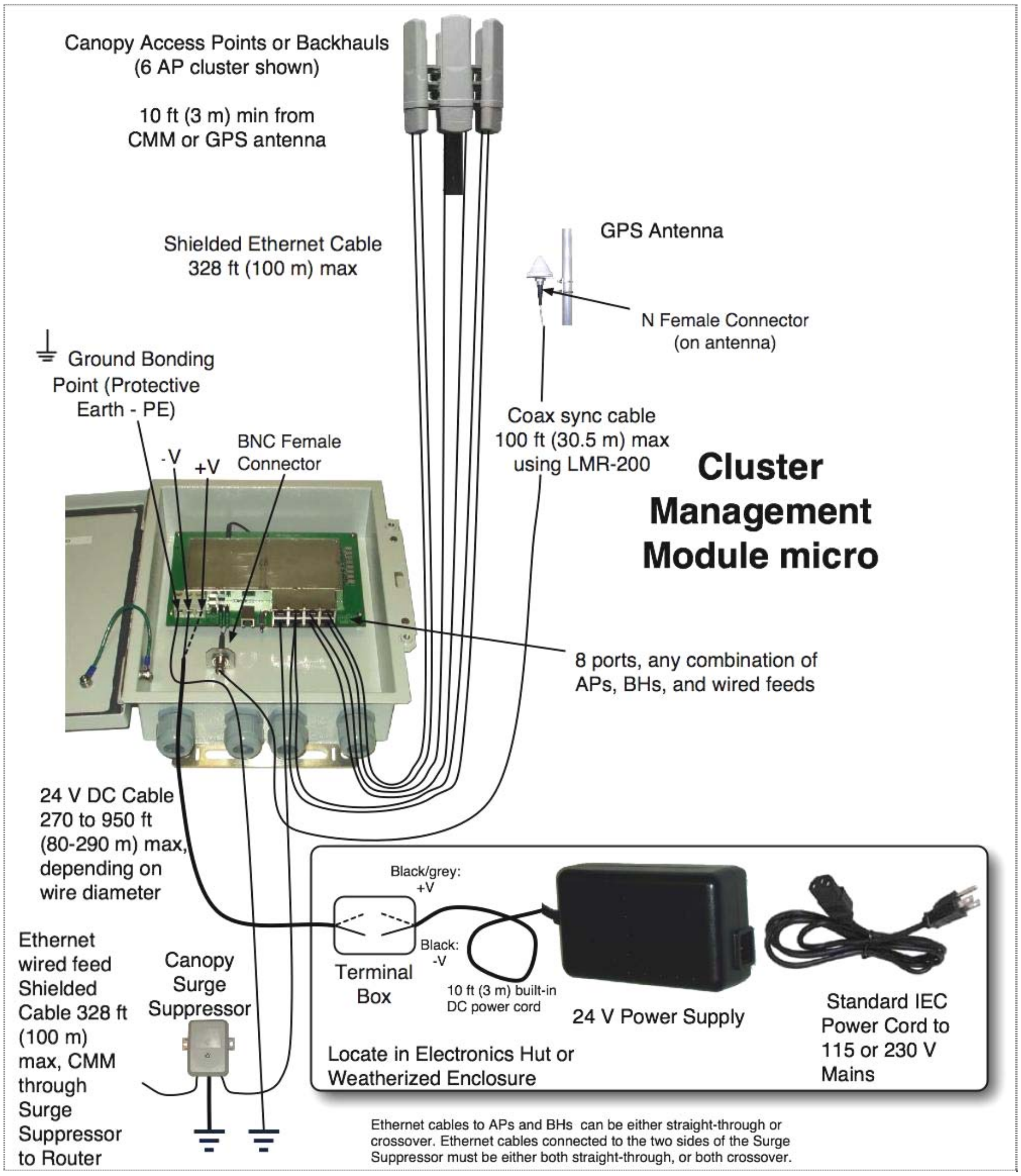


1 24 V DC power connection on terminal block (+V).
2 24 V DC ground connection on terminal block (-V).
3 Ground bonding point for CMMmicro. Ground connection on terminal block, for grounding to Protective Earth (PE) ⏚.
4 Female BNC connector for connecting to coax cable from GPS antenna.
5 Status display of eight green LEDs. The left LEDs show the number of satellites visible to the CMMmicro (1, 2, ≥ 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 69: CMMmicro circuit board

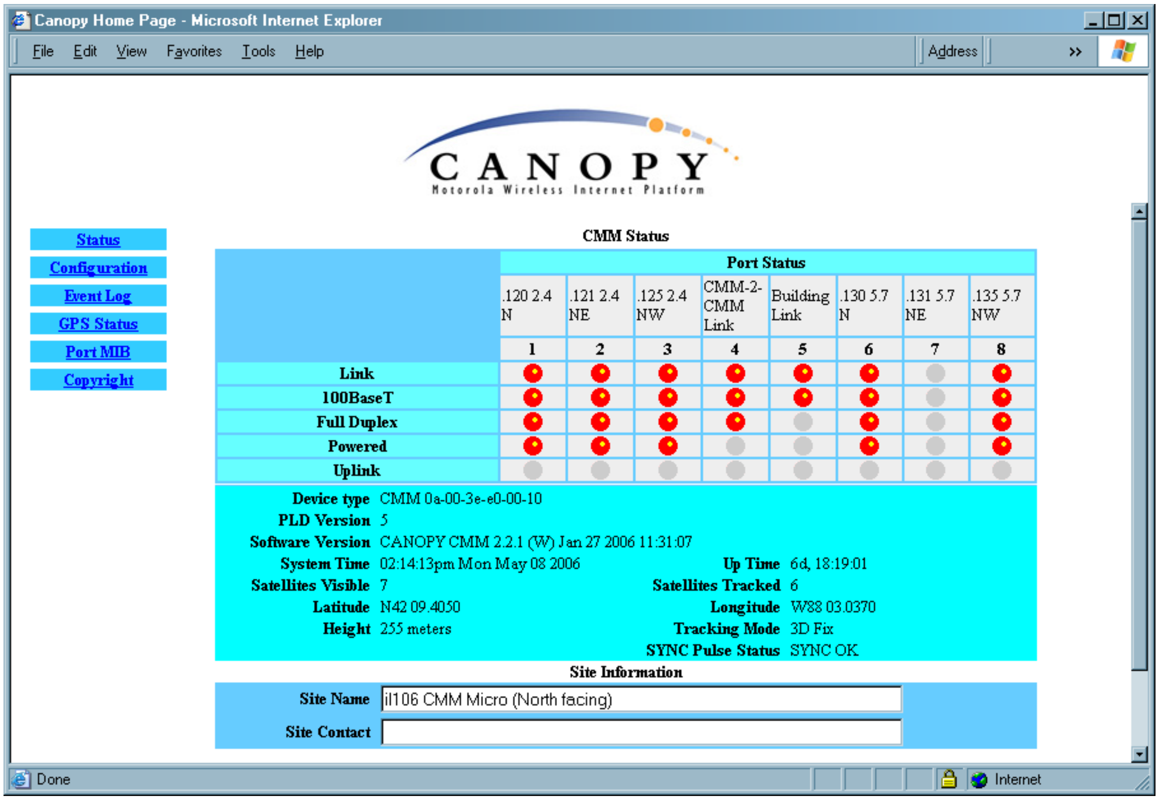


Ethernet cables to APs and BHs can be either straight-through or crossover. Ethernet cables connected to the two sides of the Surge Suppressor must be either both straight-through, or both crossover.

Figure 70: CMMmicro connections

16.5.2 Status Page of the CMMmicro

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


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

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 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 Cyclone 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 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

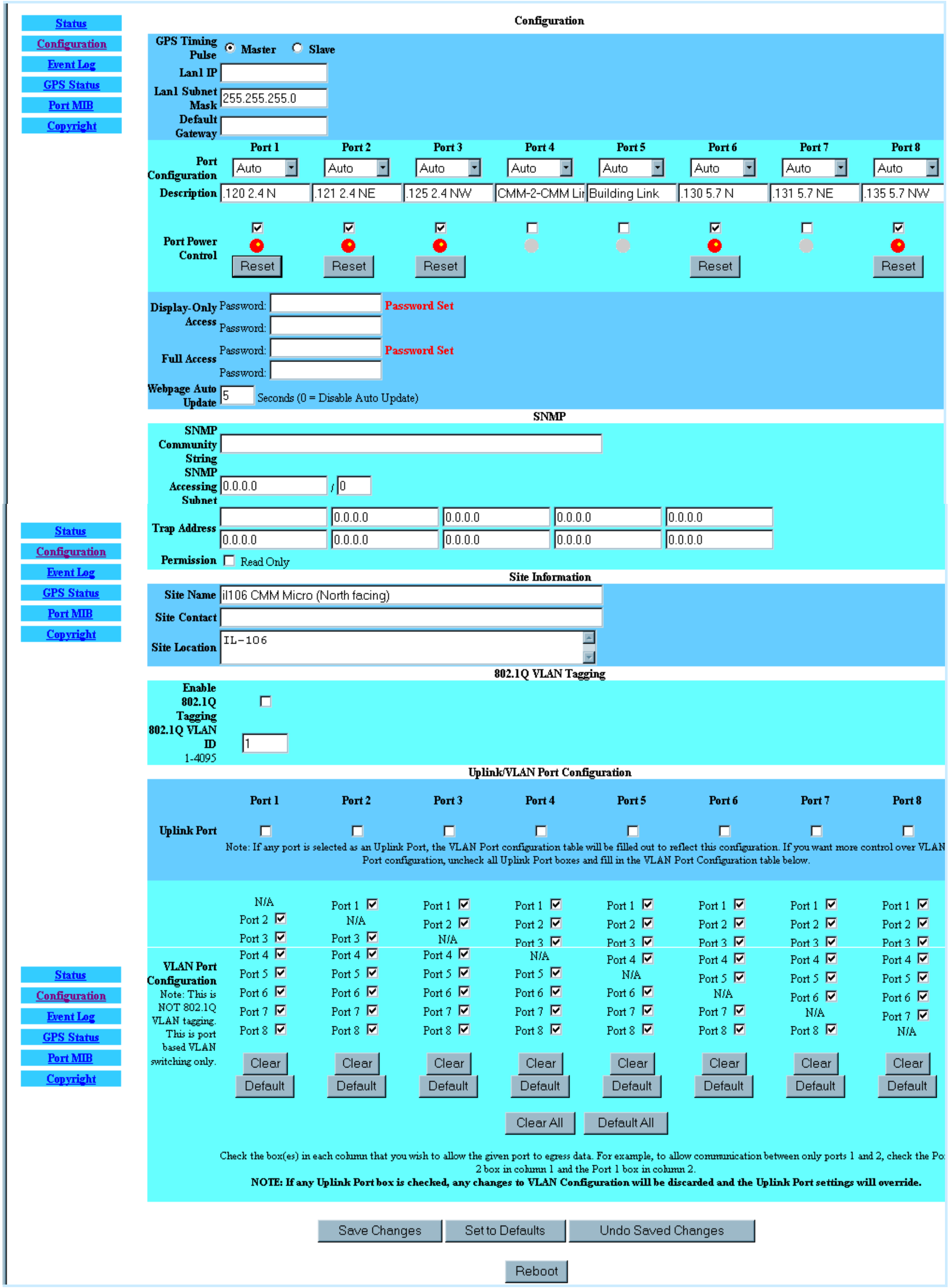
This field displays administrative information that has been entered on the Configuration page of the CMMmicro.

Site Contact

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

16.5.3 Configuration Page of the CMMmicro

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



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	☑ ● Reset	☑ ● Reset	☑ ● Reset	□ ●	□ ●	☑ ● Reset	□ ●	☑ ● Reset

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.								
	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
	Clear Default	Clear Default	Clear Default	Clear Default	Clear Default	Clear Default	Clear Default	Clear Default

Clear All Default All

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 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 381.

> *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 Cyclone APs or BHs.

> *CAUTION!*
>
> Never connect any devices other than Cyclone 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 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 381.

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 381.

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 **Cyclone**.

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.
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.

16.5.4 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

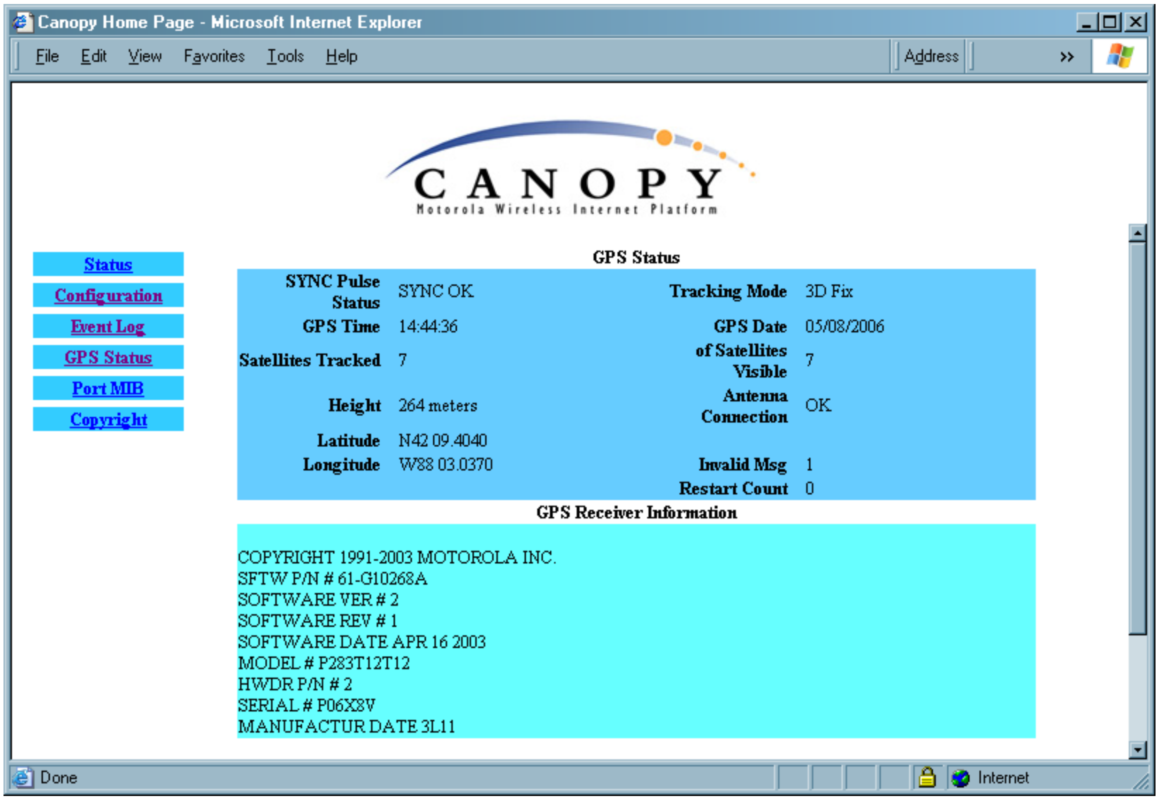
- Sync Input on Page 239.
- Sync Input on Page 299.

16.5.5 Event Log Page of the CMMmicro

This page may contain information that can be useful under the guidance of Cyclone 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.



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 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.

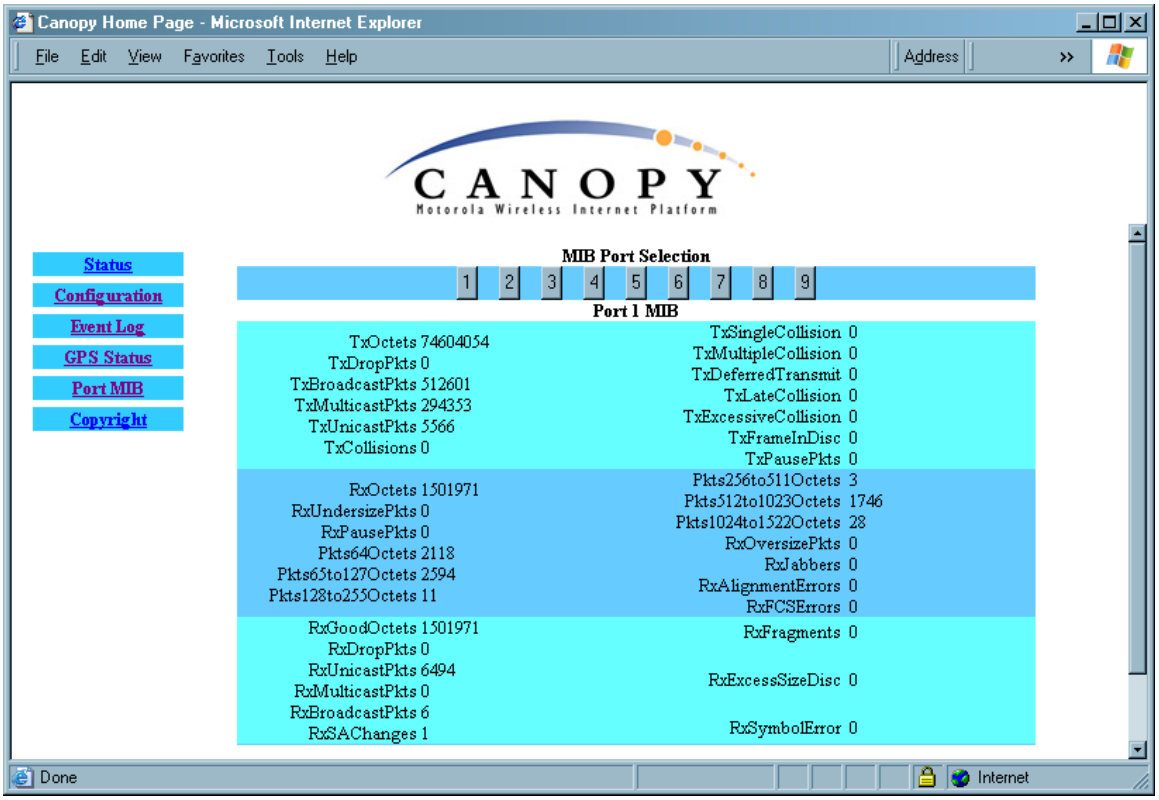
The other GPS Status fields are described under Satellites Visible on Page 223.

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.


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 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 237, 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

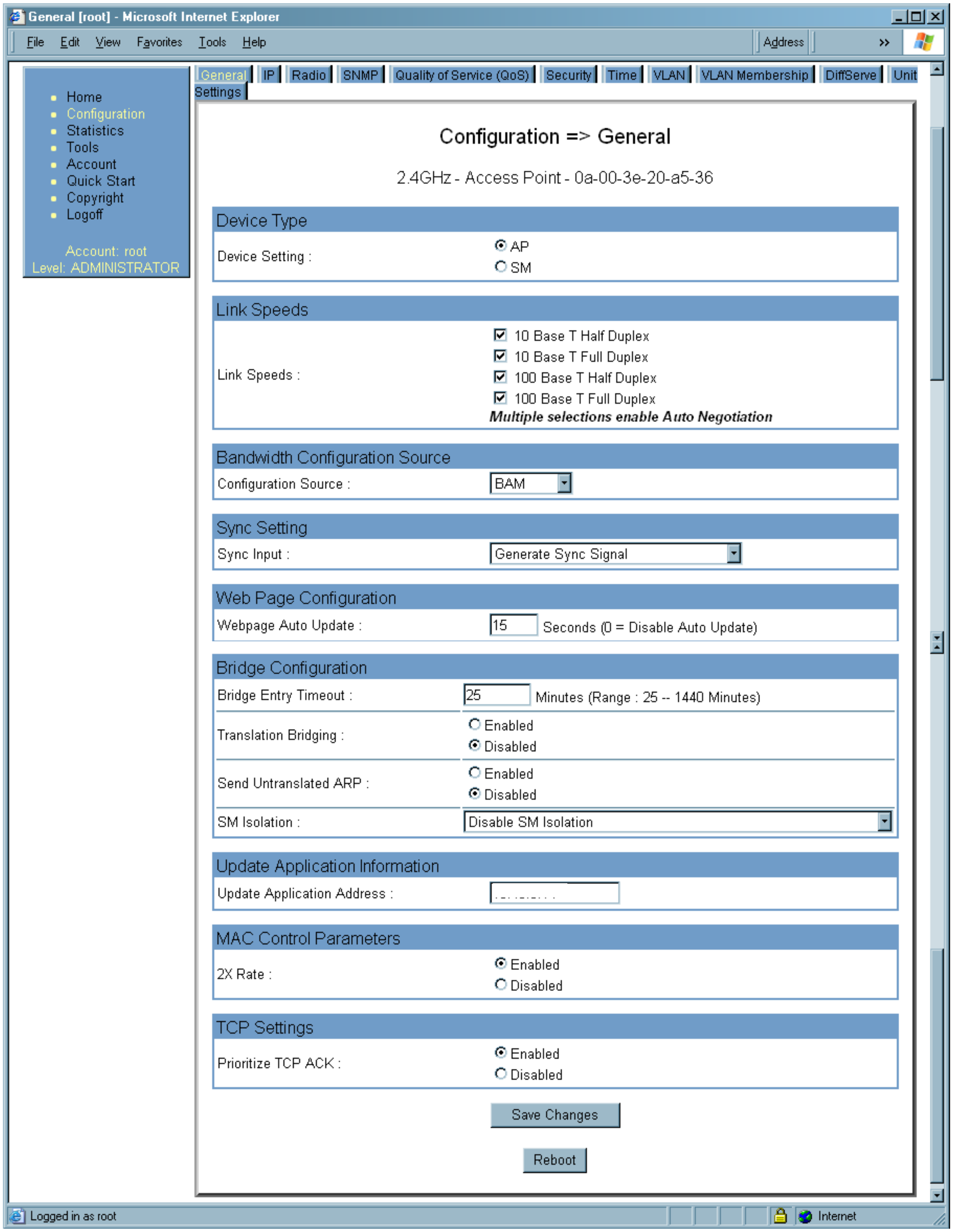
18 CONFIGURING FOR THE DESTINATION

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 377.

18.1.1 General Tab of the AP

An example of an AP General tab is displayed in Figure 75.


General [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 Settings
Home
Configuration
Statistics
Tools
Account
Quick Start
Copyright
Logoff
Account: root
Level: ADMINISTRATOR
Save Changes
Reboot
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

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 370. 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 295.

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 90.

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.

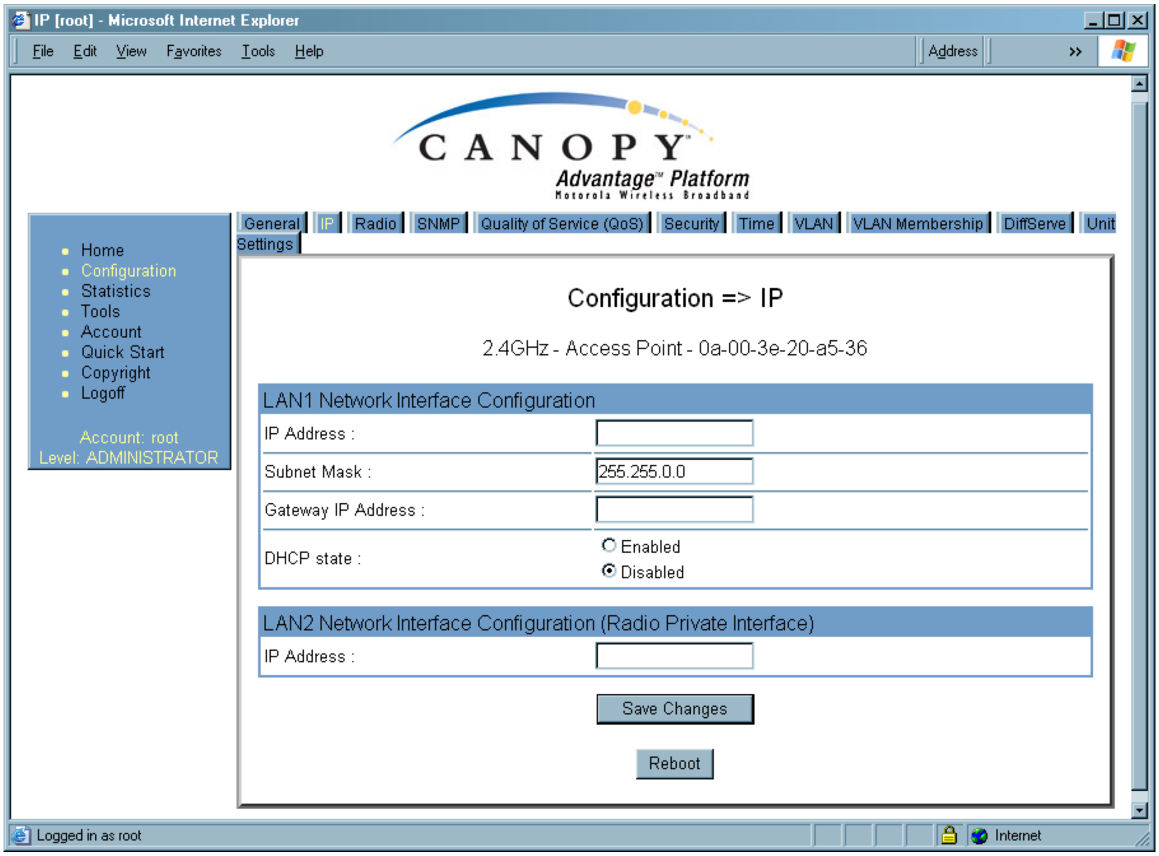
Reboot

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.



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 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 381.

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.

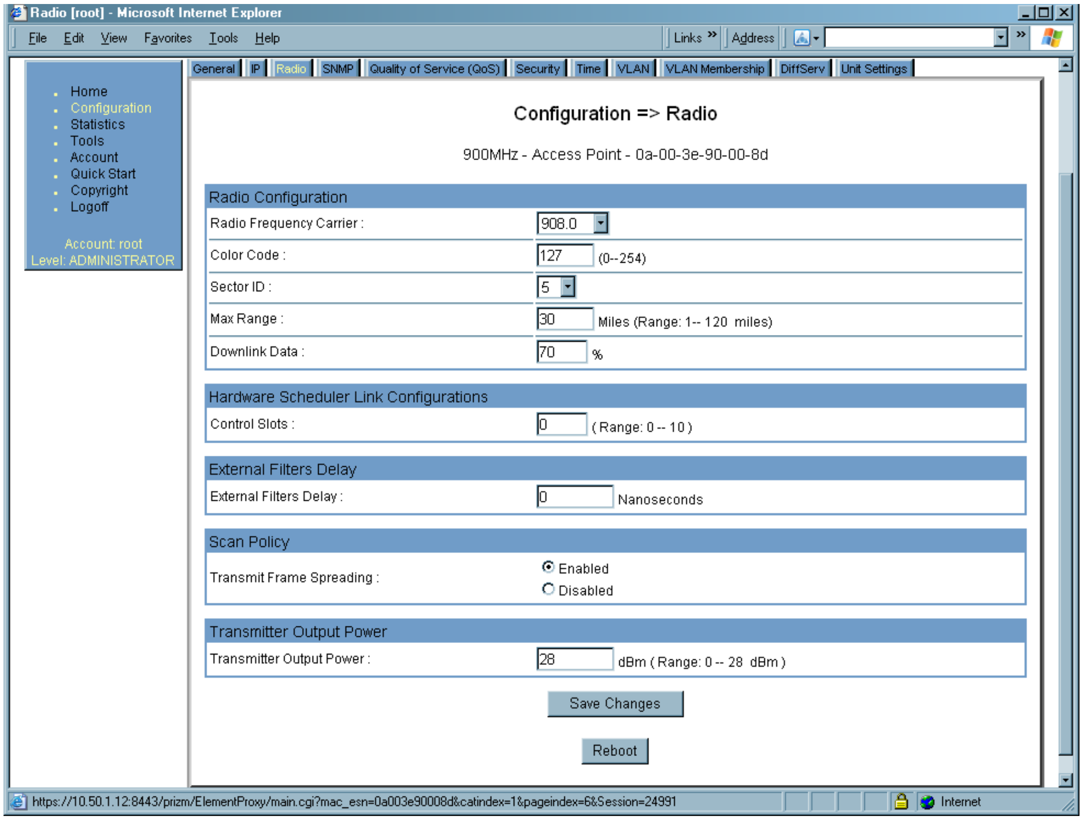
Reboot

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.


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 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 Cyclone 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 Cyclone 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[6] 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 444.

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.

[6] See Noting Possible Obstructions in the Fresnel Zone on Page 67.

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 Cyclone 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 330.

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.

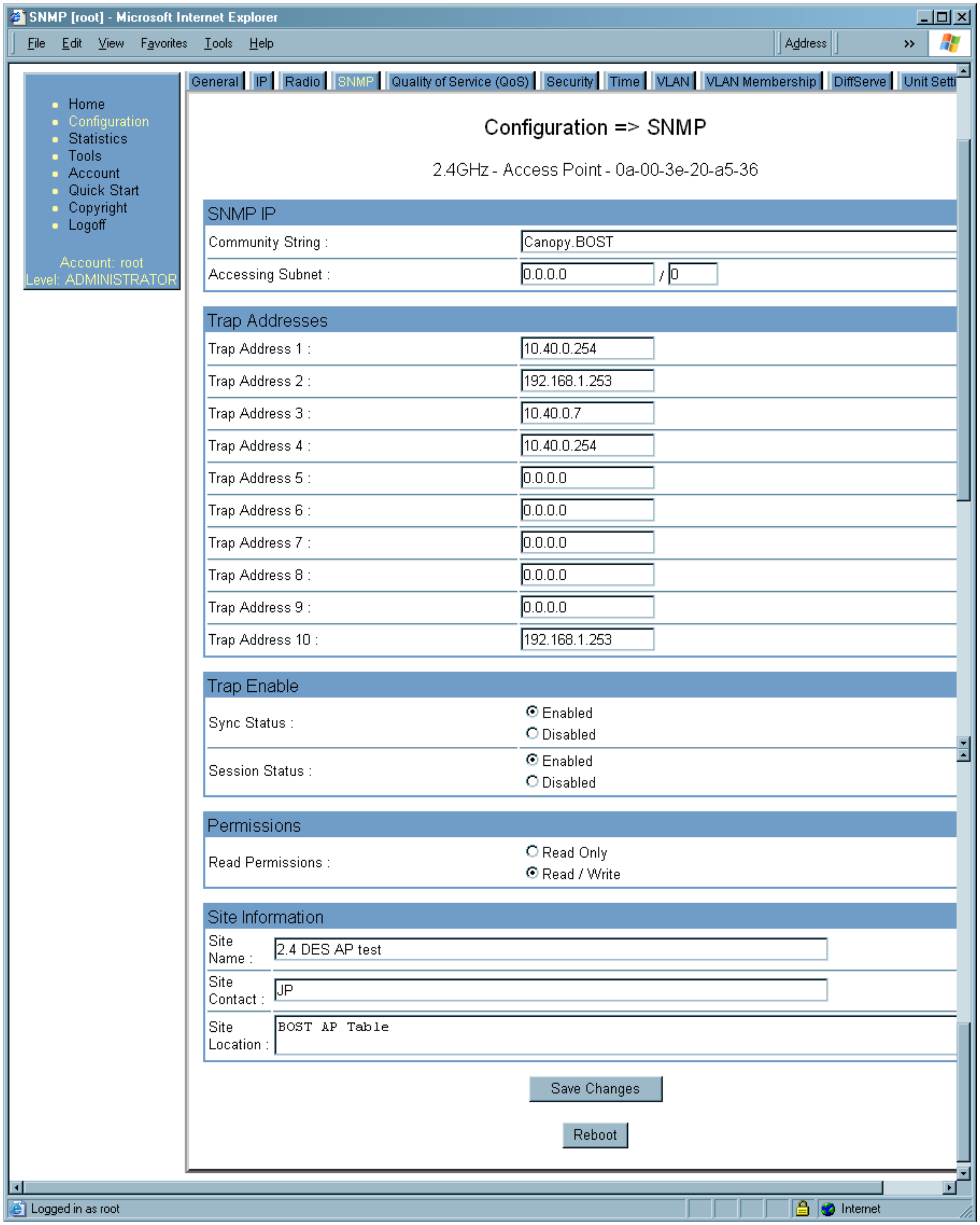
Reboot

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.



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
Logged in as root
Internet

Account: root
Level: ADMINISTRATOR

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 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 **Cyclone**.

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 Cyclone Enterprise MIB on Page 410. 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.

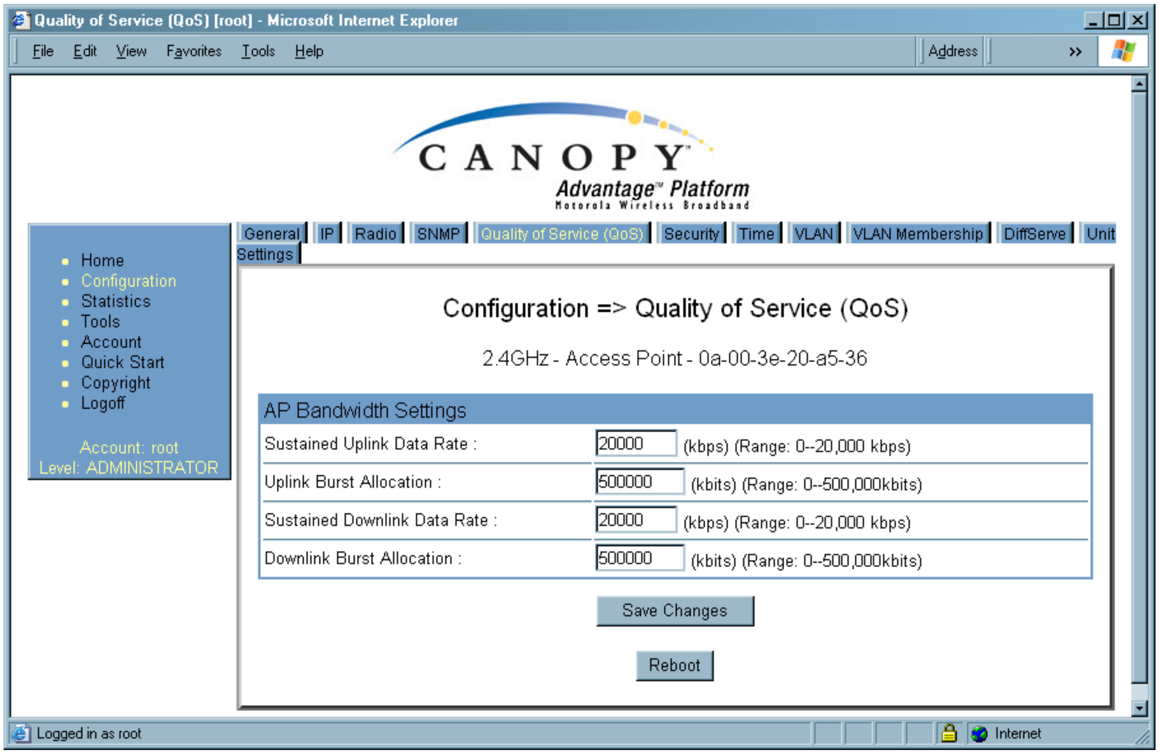
Reboot

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.



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 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 295.

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 295.

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 295.

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 295.

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.

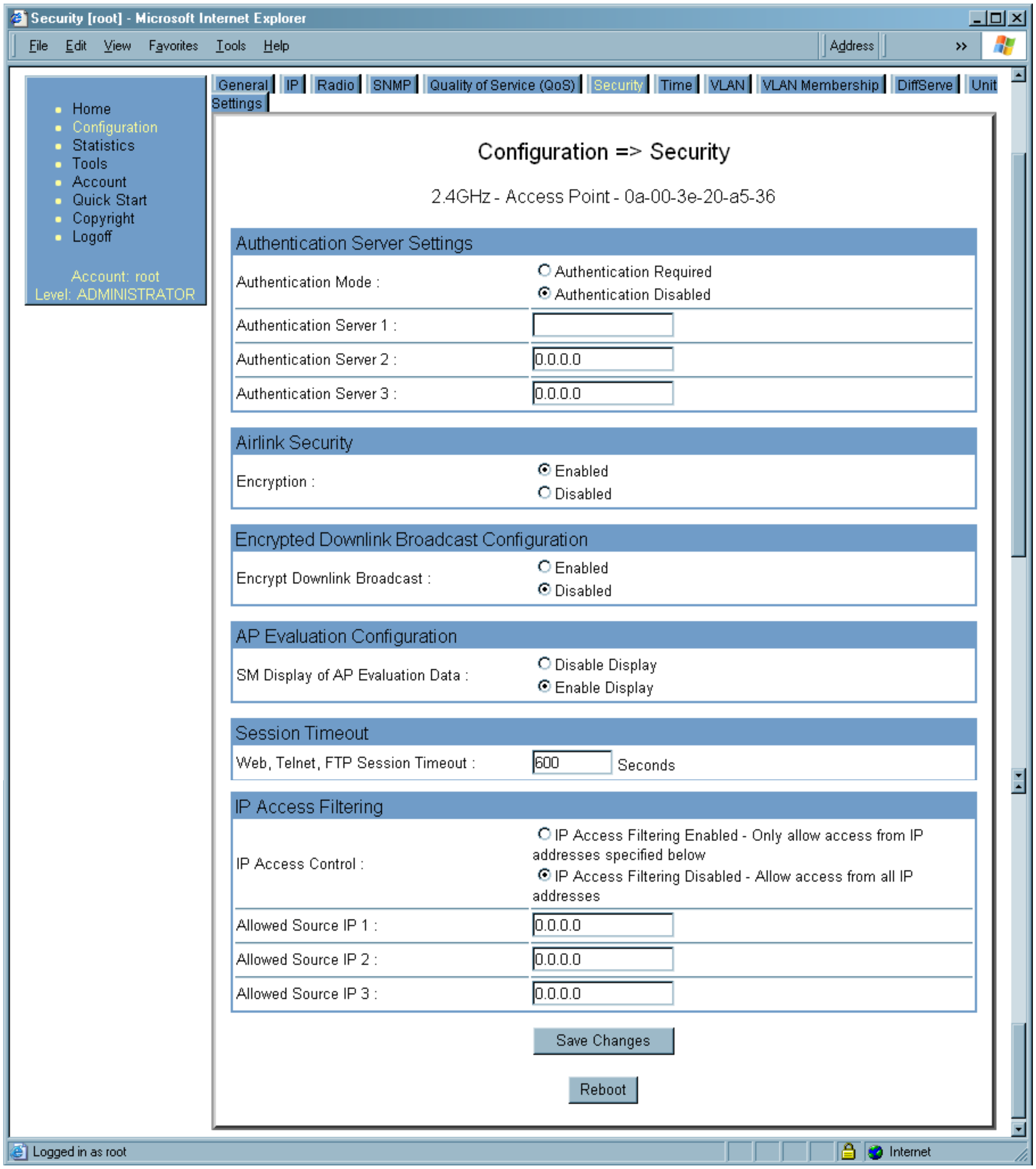
Reboot

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.



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 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 384.

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.

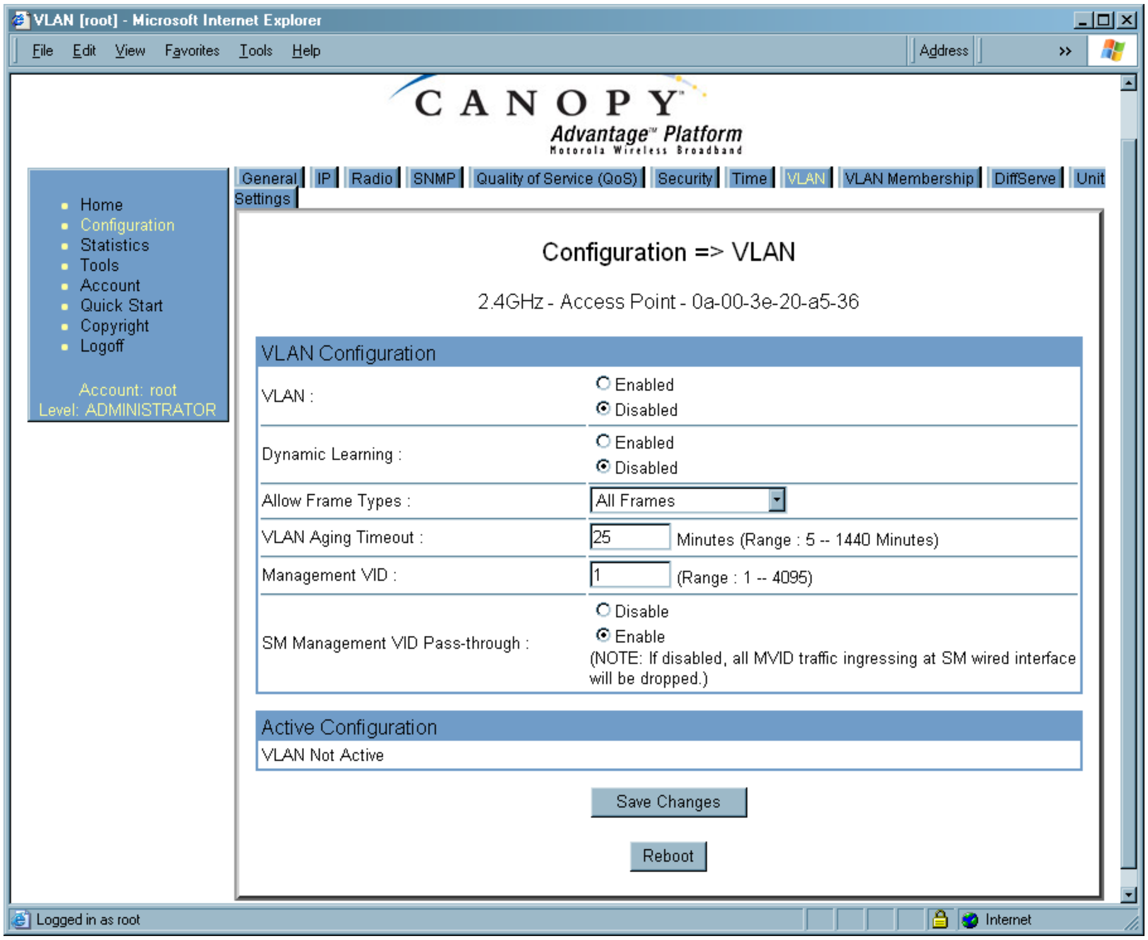
Reboot

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.


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 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.

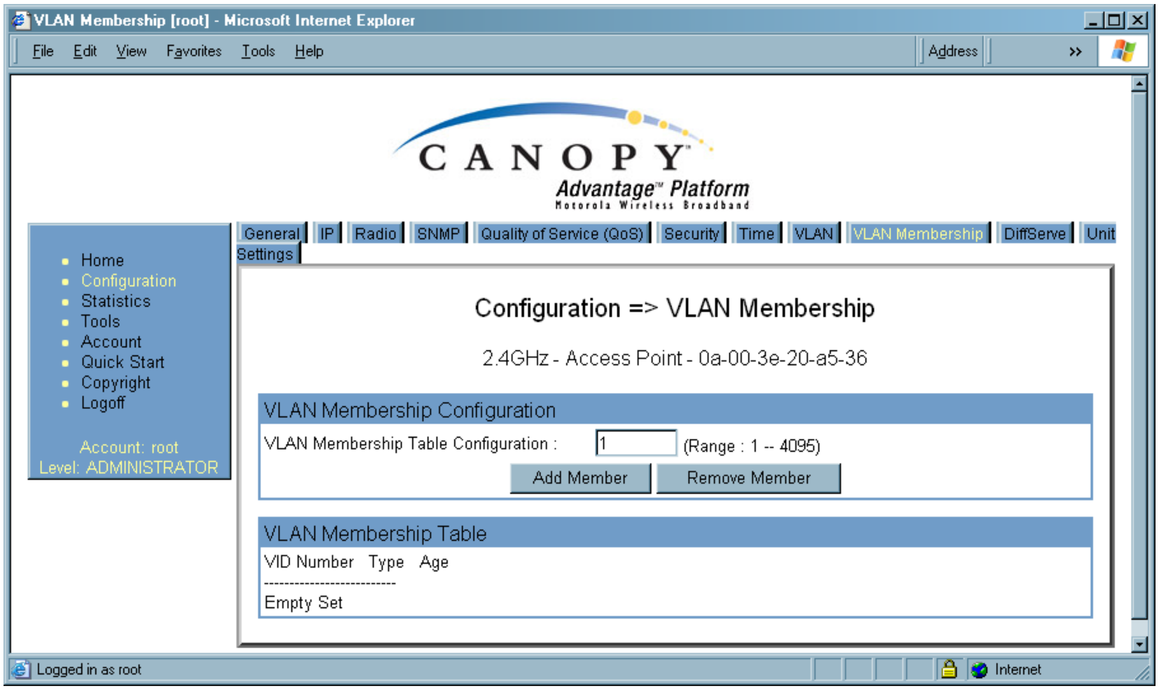
Reboot

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.



Account: root
Level: ADMINISTRATOR

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 82: VLAN Membership tab of AP, example

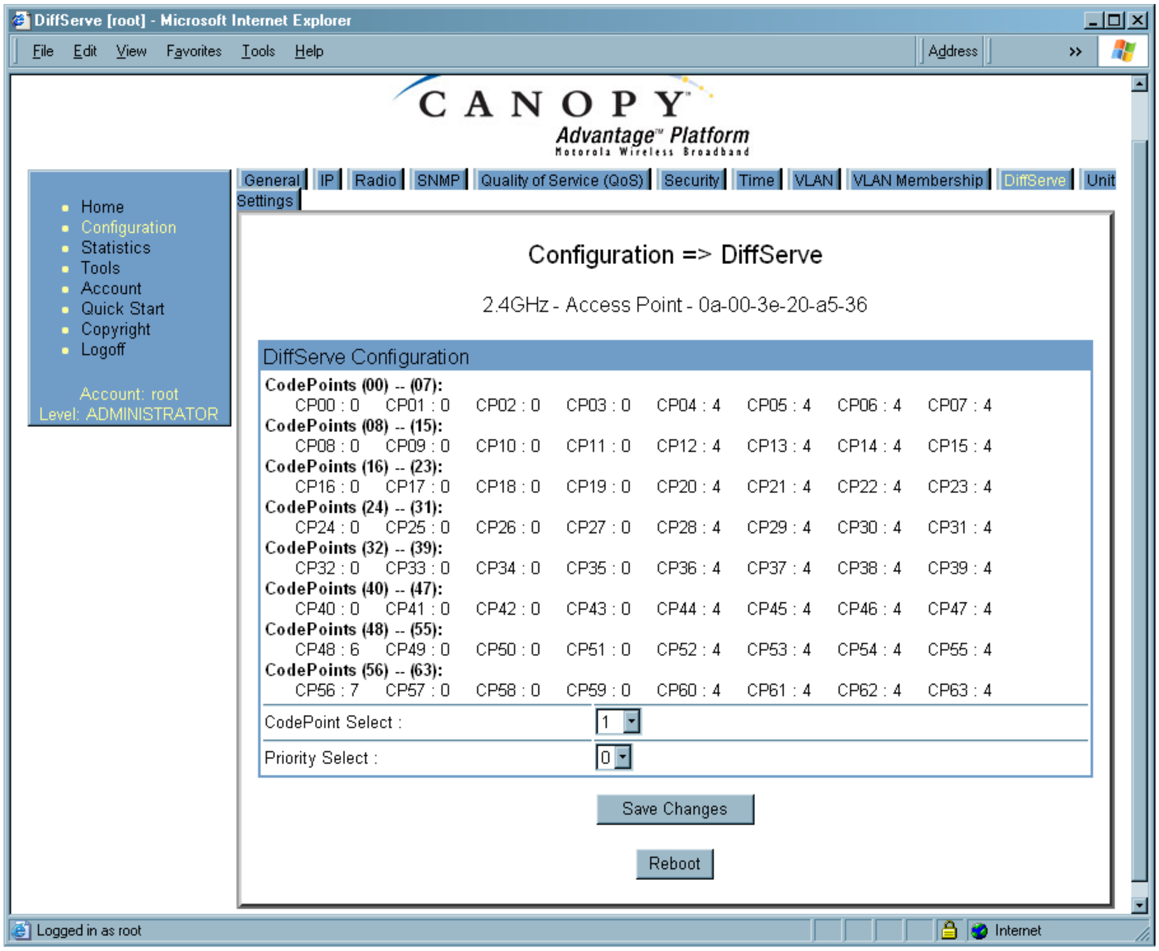
You may set the VLAN Membership tab parameter as follows.

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.



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

Figure 83: 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 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).

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.

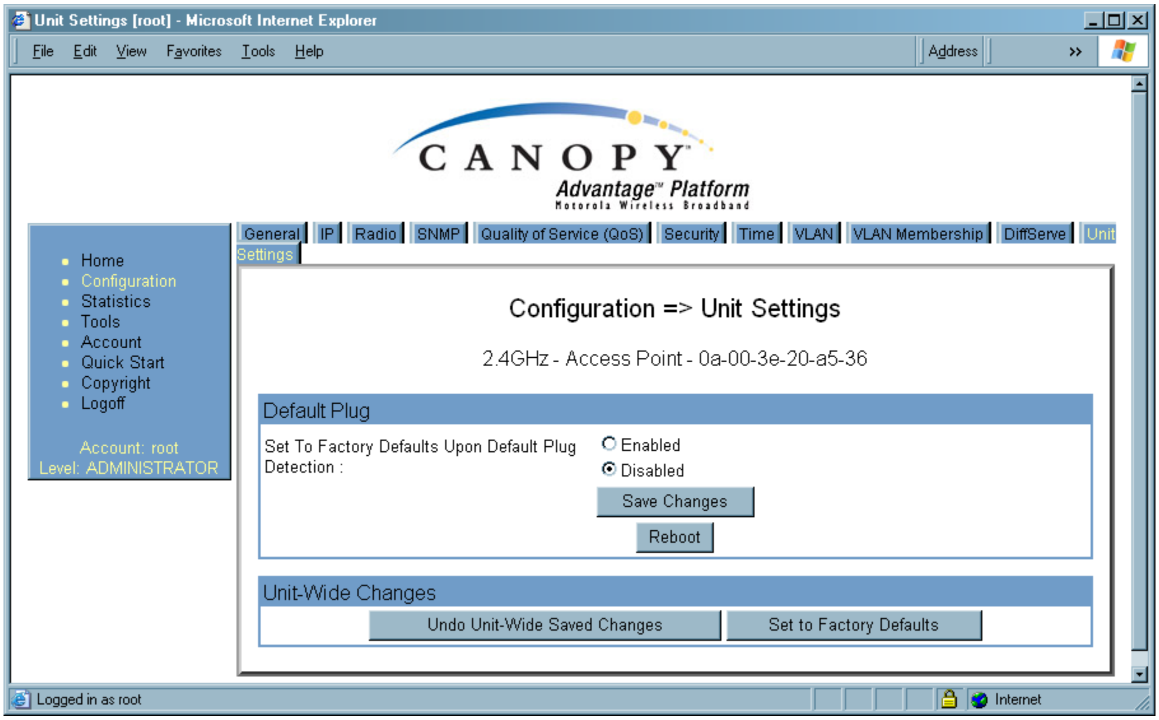
Reboot

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.



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 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 379.

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

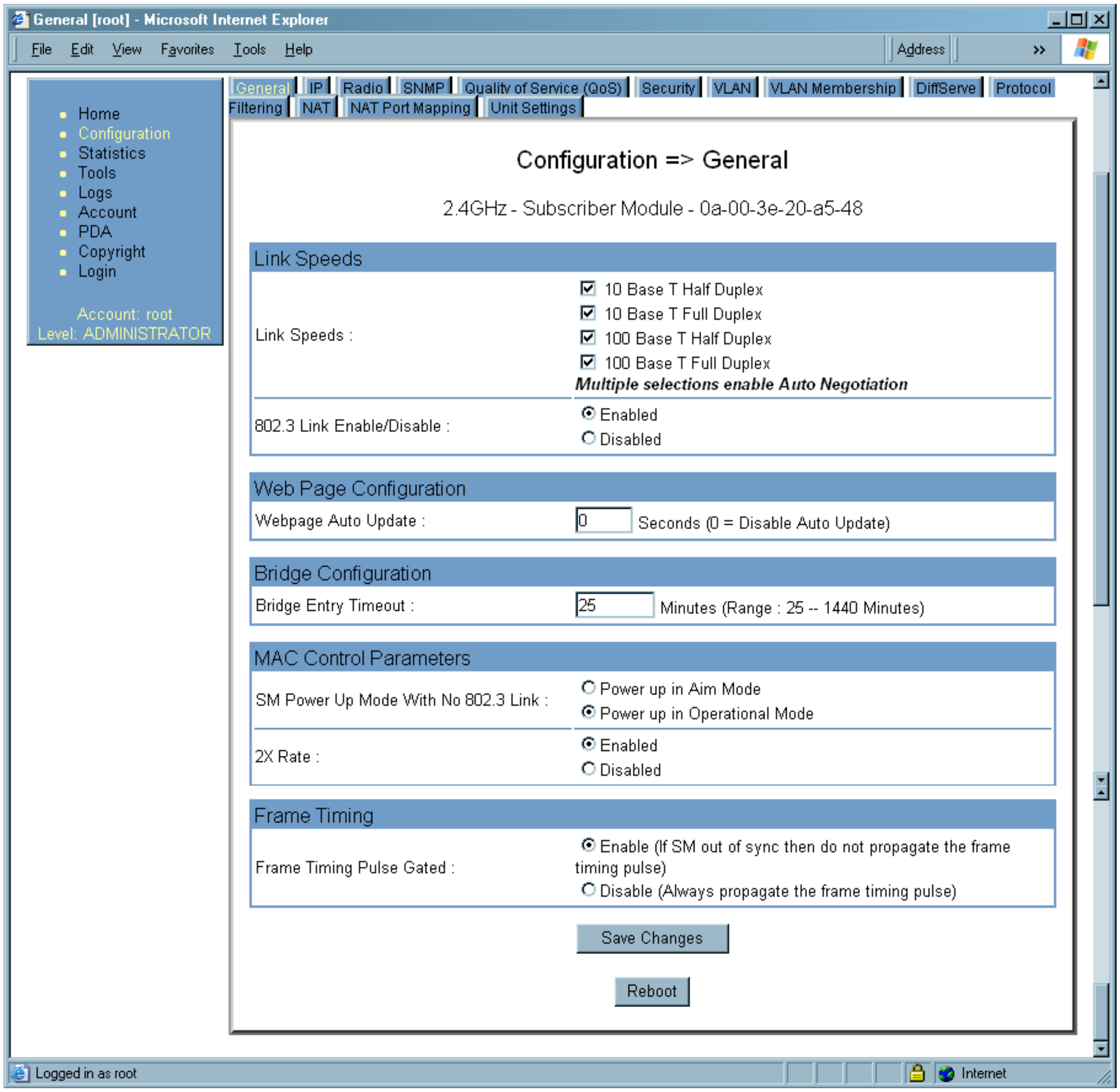
When you click this button, *all configurable parameters on all tabs* are reset to the factory settings.

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 377.

18.2.1 General Tab of the SM

An example of a General tab in the SM is displayed in Figure 85.


General [root] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address
General | IP | Radio | SNMP | Quality of Service (QoS) | Security | VLAN | VLAN Membership | DiffServe | Protocol Filtering | NAT | NAT Port Mapping | Unit Settings
Home
Configuration
Statistics
Tools
Logs
Account
PDA
Copyright
Login
Account: root
Level: ADMINISTRATOR
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 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 90.

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 374.

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.

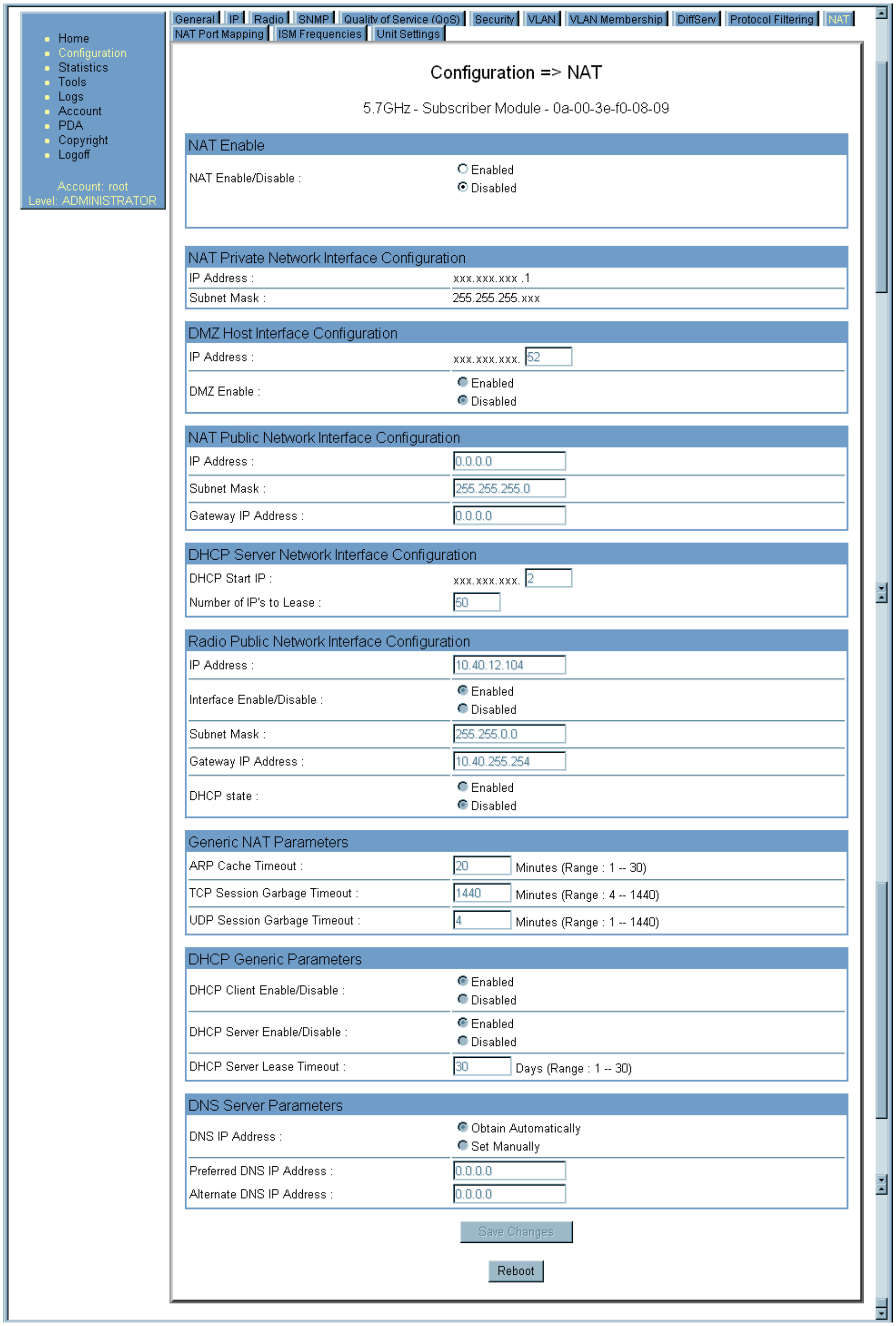
Reboot

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 - 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 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 271.

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

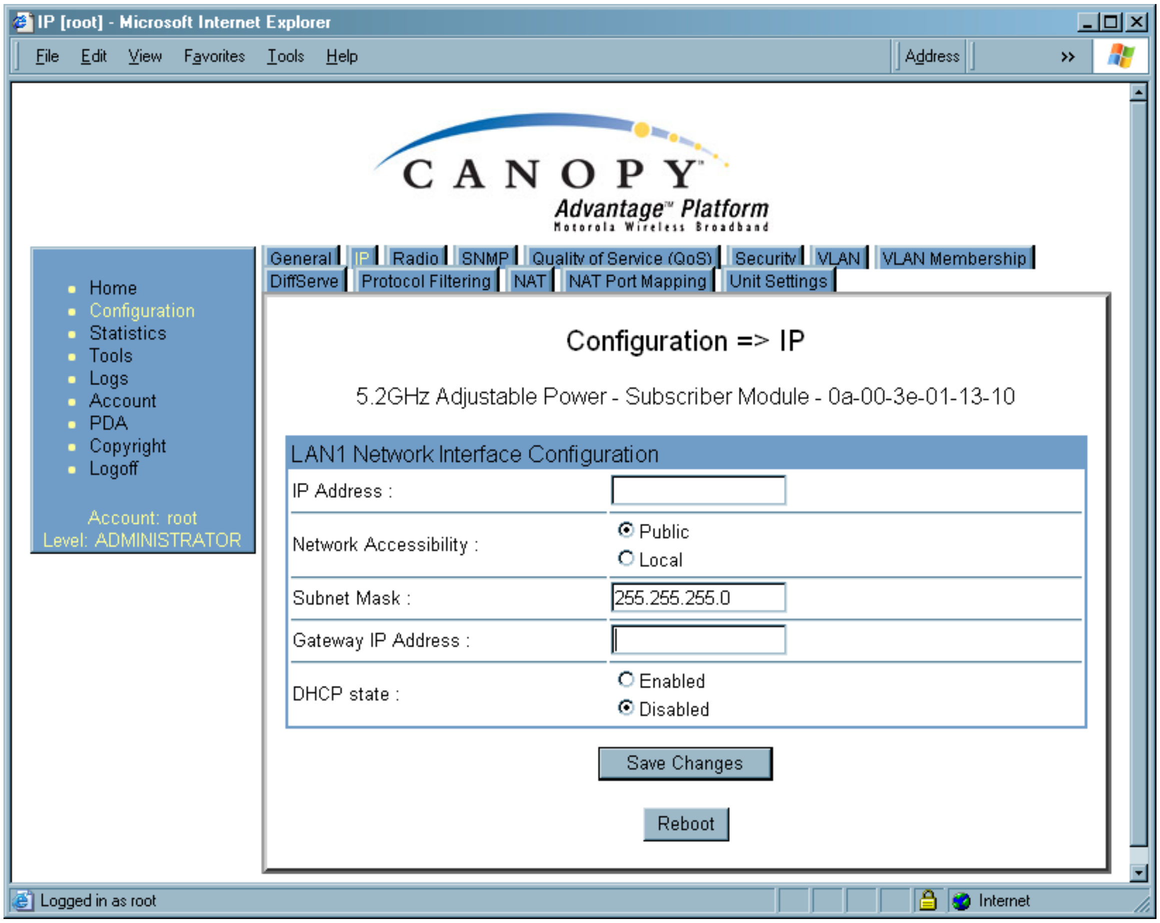
When you click this button, any changes that you made on all tabs are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

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.



Account: root
Level: ADMINISTRATOR

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

Logged in as root

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 381.

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.

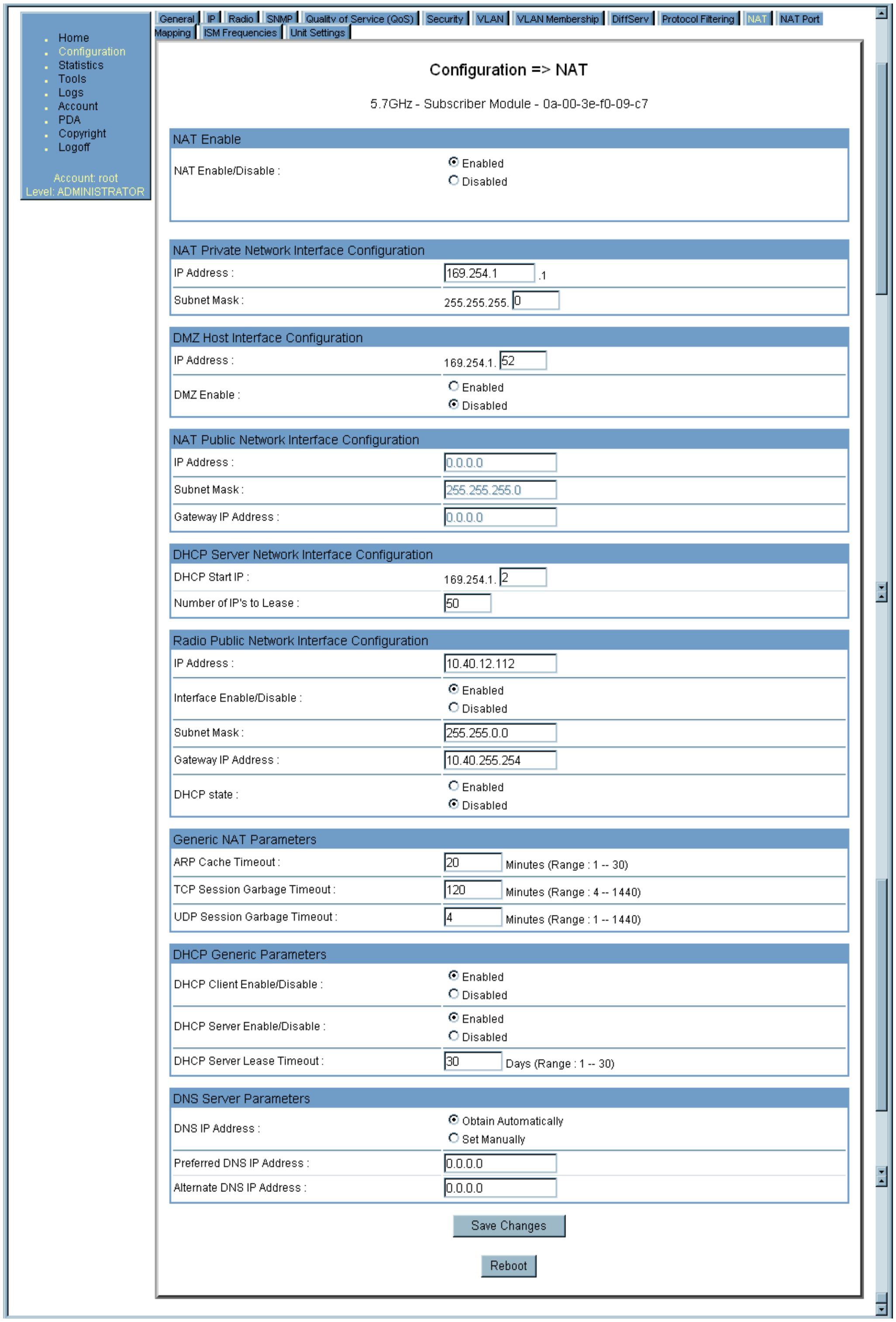
Reboot

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.



Home
Configuration
Statistics
Tools
Logs
Account
PDA
Copyright
Logoff
Account: root
Level: ADMINISTRATOR
General | IP | Radio | SNMP | Quality of Service (QoS) | Security | VLAN | VLAN Membership | DiffServ | Protocol Filtering | NAT | NAT Port Mapping | ISM Frequencies | Unit Settings

Configuration => NAT

5.7GHz - Subscriber Module - 0a-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 :	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 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 271.

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

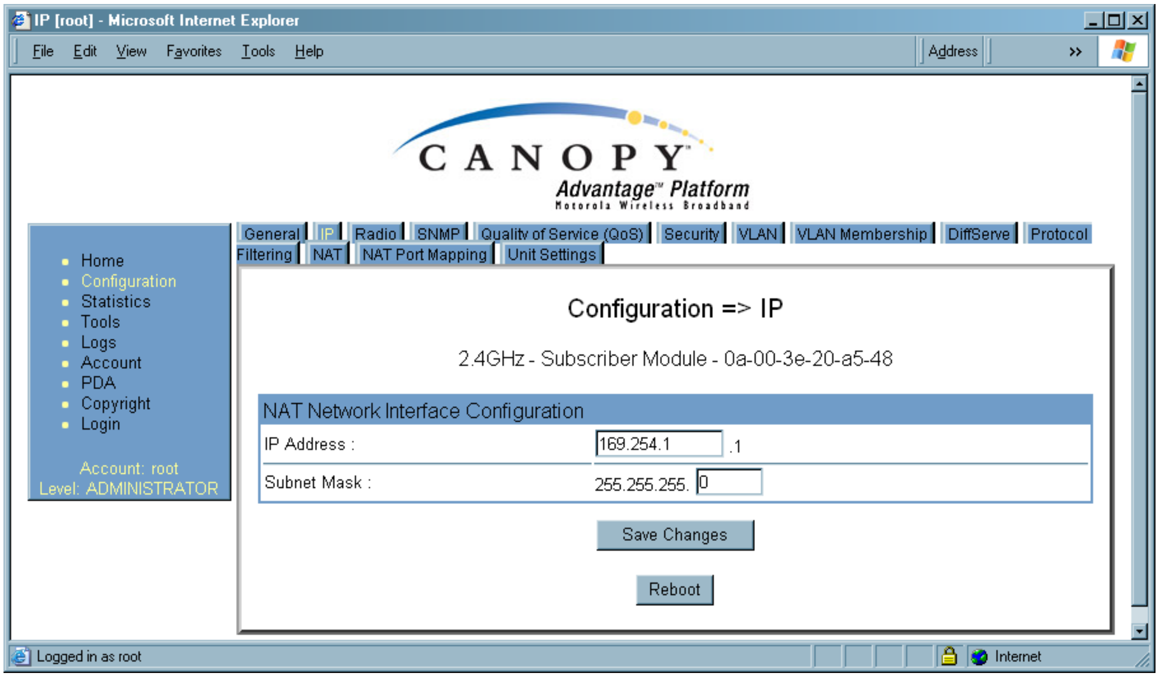
When you click this button, any changes that you made on all tabs are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

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.



Configuration => IP

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

NAT Network Interface Configuration

IP Address : 169.254.1 .1

Subnet Mask : 255.255.255. 0

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

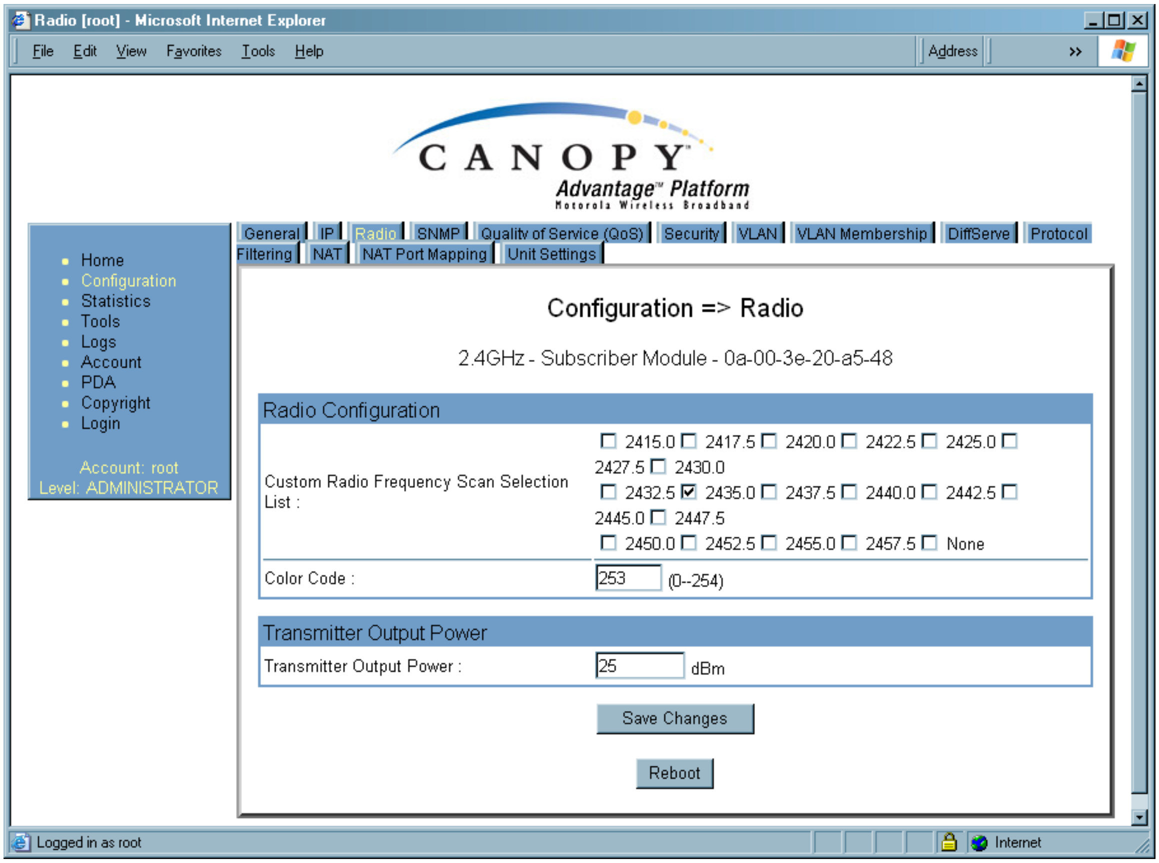
When you click this button

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.



Configuration => Radio

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

Radio Configuration

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

Color Code : 253 (0--254)

Transmitter Output Power

Transmitter Output Power : 25 dBm

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 Cyclone 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 Cyclone 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 330.

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.

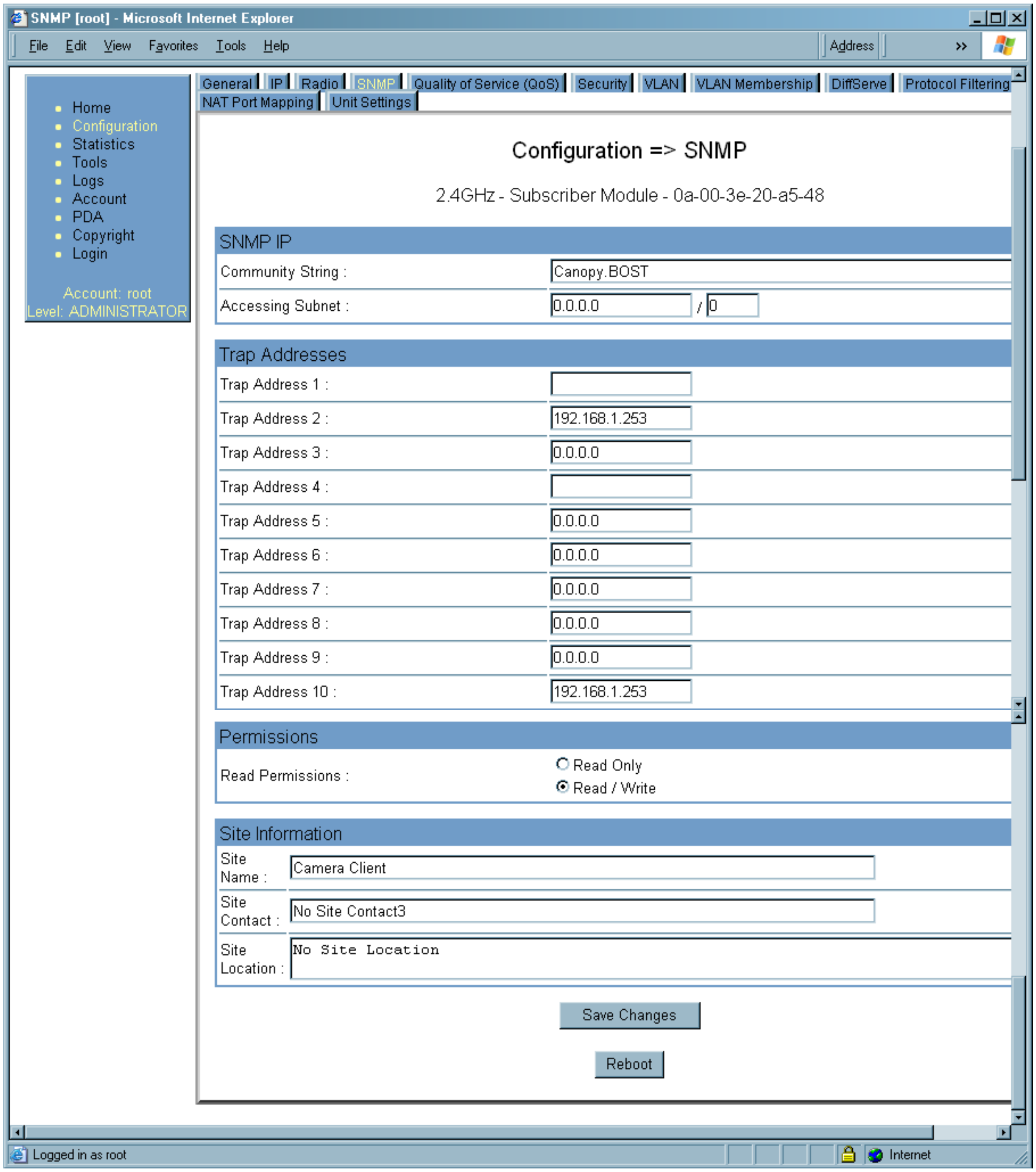
Reboot

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 DiffServe Protocol Filtering
NAT Port Mapping Unit Settings
Home
Configuration
Statistics
Tools
Logs
Account
PDA
Copyright
Login
Account: root
Level: ADMINISTRATOR
Save Changes
Reboot
Logged in as root
Internet

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

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 **Cyclone**.

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 382.

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.

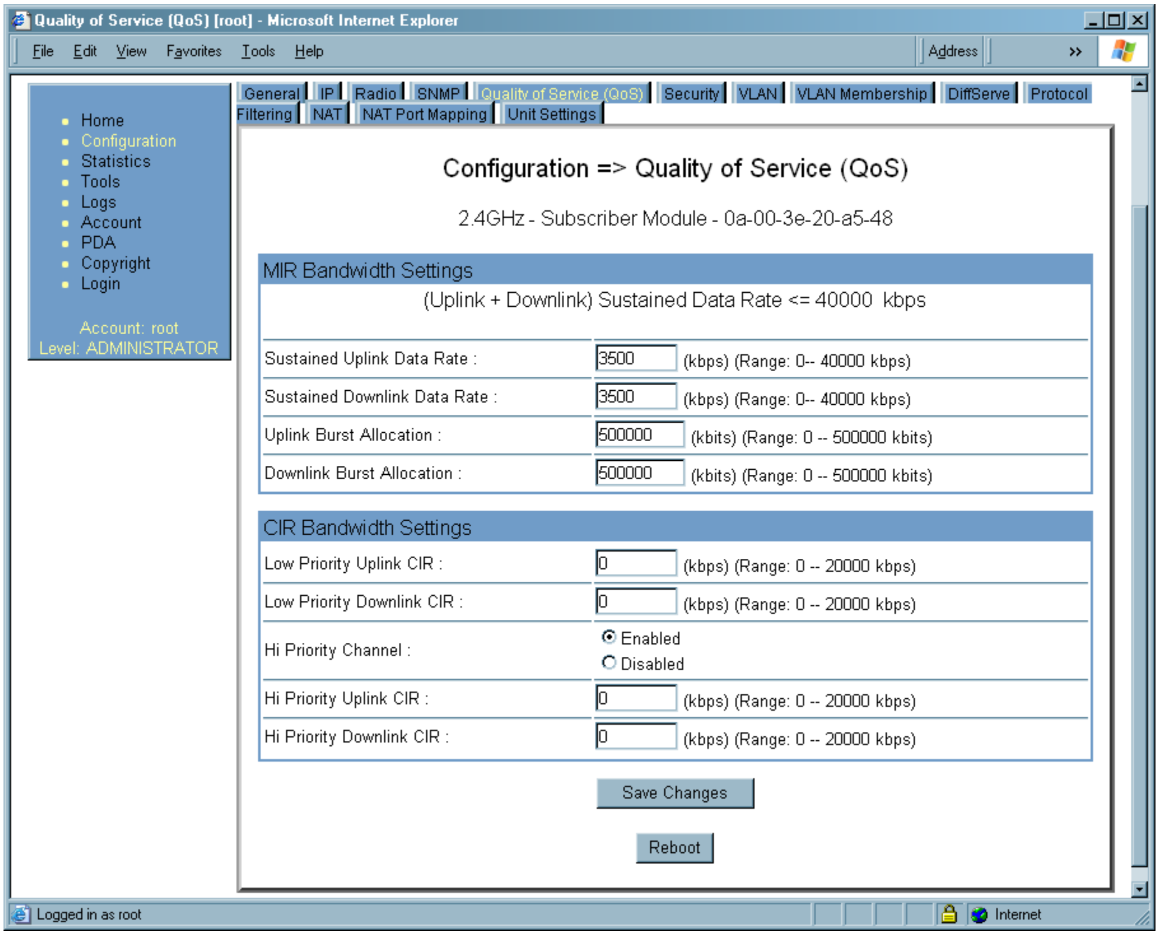
Reboot

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.


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

Configuration => Quality of Service (QoS)

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

MIR Bandwidth Settings

(Uplink + Downlink) Sustained Data Rate <= 40000 kbps

Sustained Uplink Data Rate :	3500 (kbps) (Range: 0-- 40000 kbps)
Sustained Downlink Data Rate :	3500 (kbps) (Range: 0-- 40000 kbps)
Uplink Burst Allocation :	500000 (kbits) (Range: 0 -- 500000 kbits)
Downlink Burst Allocation :	500000 (kbits) (Range: 0 -- 500000 kbits)

CIR Bandwidth Settings

Low Priority Uplink CIR :	0 (kbps) (Range: 0 -- 20000 kbps)
Low Priority Downlink CIR :	0 (kbps) (Range: 0 -- 20000 kbps)
Hi Priority Channel :	● Enabled ○ Disabled
Hi Priority Uplink CIR :	0 (kbps) (Range: 0 -- 20000 kbps)
Hi Priority Downlink CIR :	0 (kbps) (Range: 0 -- 20000 kbps)

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 295.

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 295.

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 295.

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 295.

Low Priority Uplink CIR

See

- Committed Information Rate on Page 86
- Setting the Configuration Source on Page 295.

Low Priority Downlink CIR

See

- Committed Information Rate on Page 86
- Setting the Configuration Source on Page 295.

Hi Priority Channel

See

- High-priority Bandwidth on Page 86
- Setting the Configuration Source on Page 295.

Hi Priority Uplink CIR

See

- High-priority Bandwidth on Page 86
- Committed Information Rate on Page 86
- Setting the Configuration Source on Page 295.

Hi Priority Downlink CIR

See

- High-priority Bandwidth on Page 86
- Committed Information Rate on Page 86
- Setting the Configuration Source on Page 295.

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.

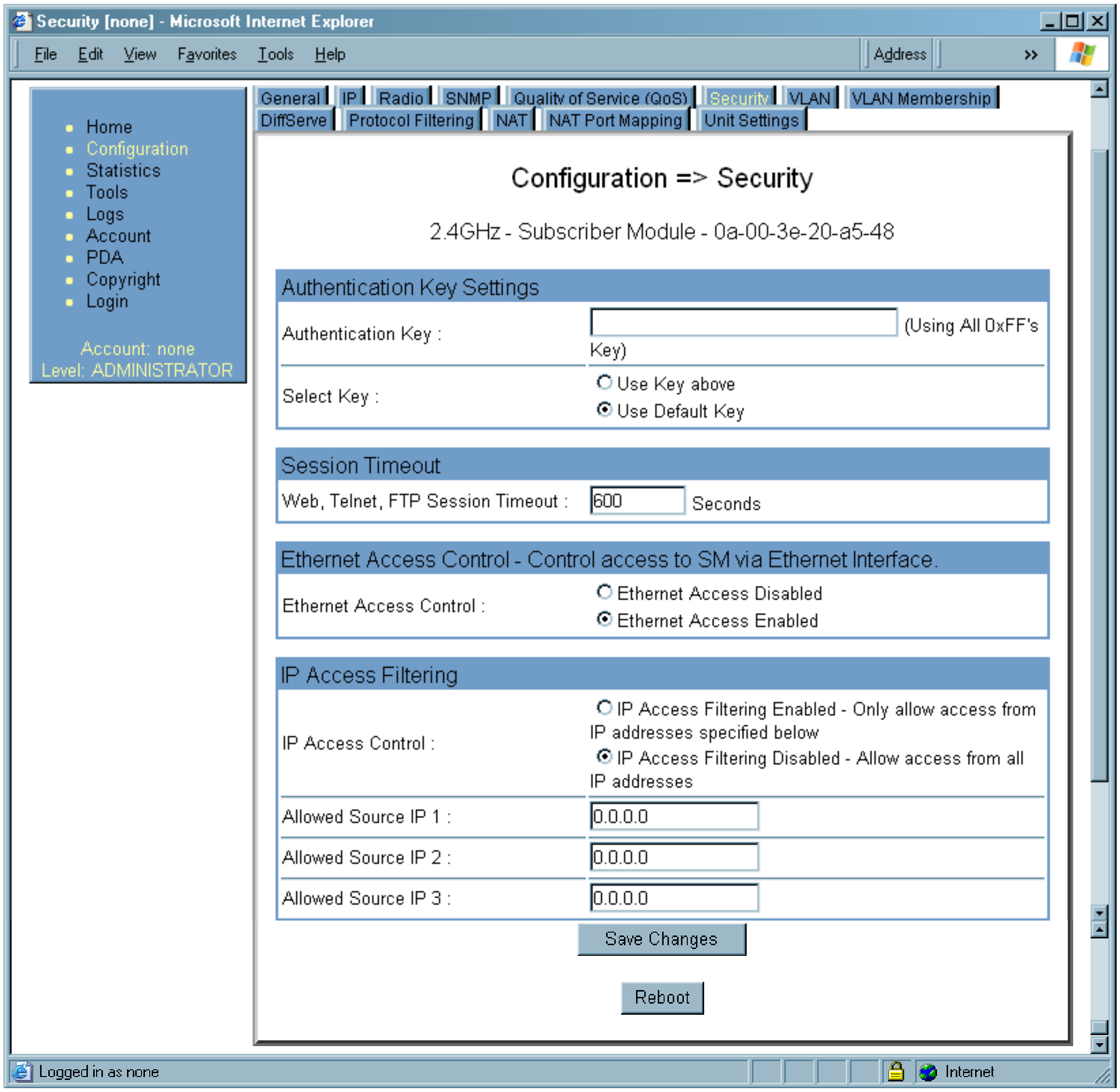
Reboot

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.



Account: none
Level: ADMINISTRATOR

Configuration => Security

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

Authentication Key Settings

Authentication Key : [ ] (Using All 0xFF's Key)

Select Key : ○ Use Key above ● Use Default Key

Session Timeout

Web, Telnet, FTP Session Timeout : 600 Seconds

Ethernet Access Control - Control access to SM via Ethernet Interface.

Ethernet Access Control : ○ Ethernet Access Disabled ● Ethernet Access Enabled

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 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 389.

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, Cyclone 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.

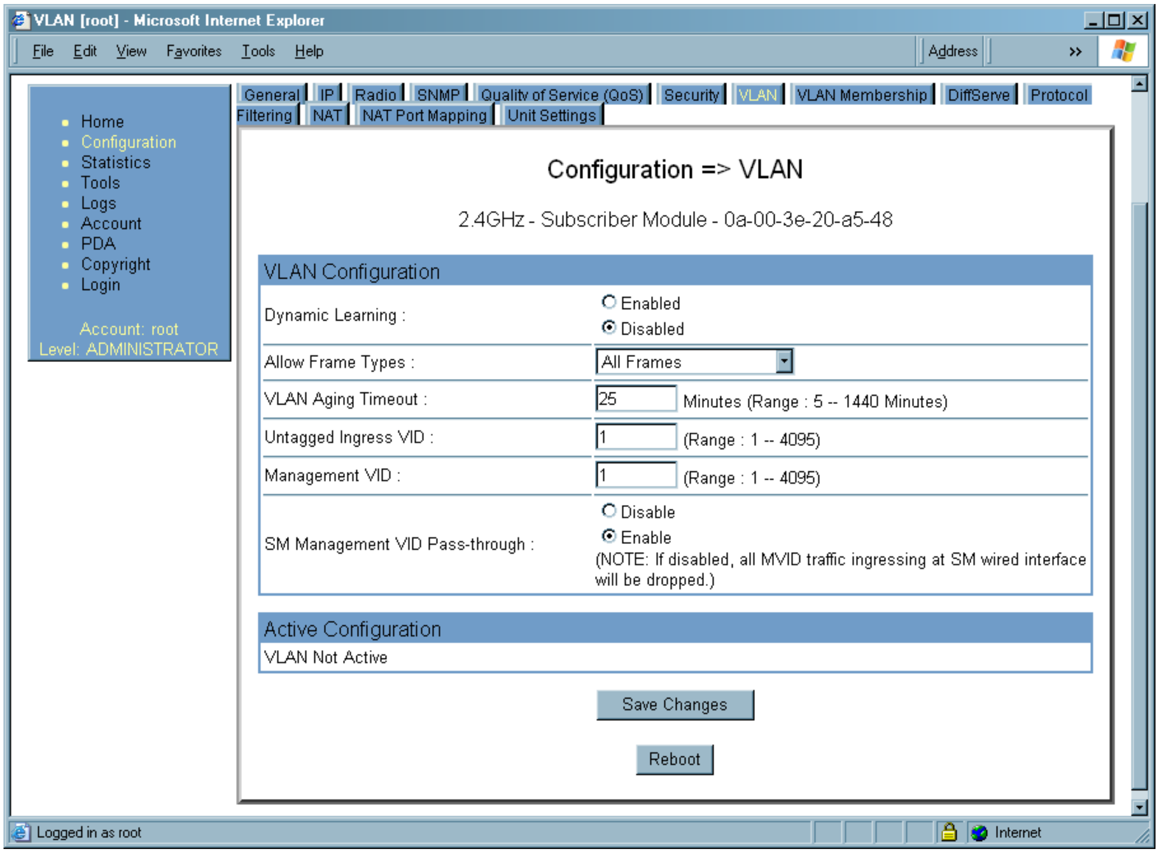
Reboot

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.


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

Configuration => VLAN

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

VLAN Configuration

Dynamic Learning :	○ Enabled ● Disabled
Allow Frame Types :	All Frames
VLAN Aging Timeout :	25 Minutes (Range : 5 -- 1440 Minutes)
Untagged Ingress VID :	1 (Range : 1 -- 4095)
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 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.

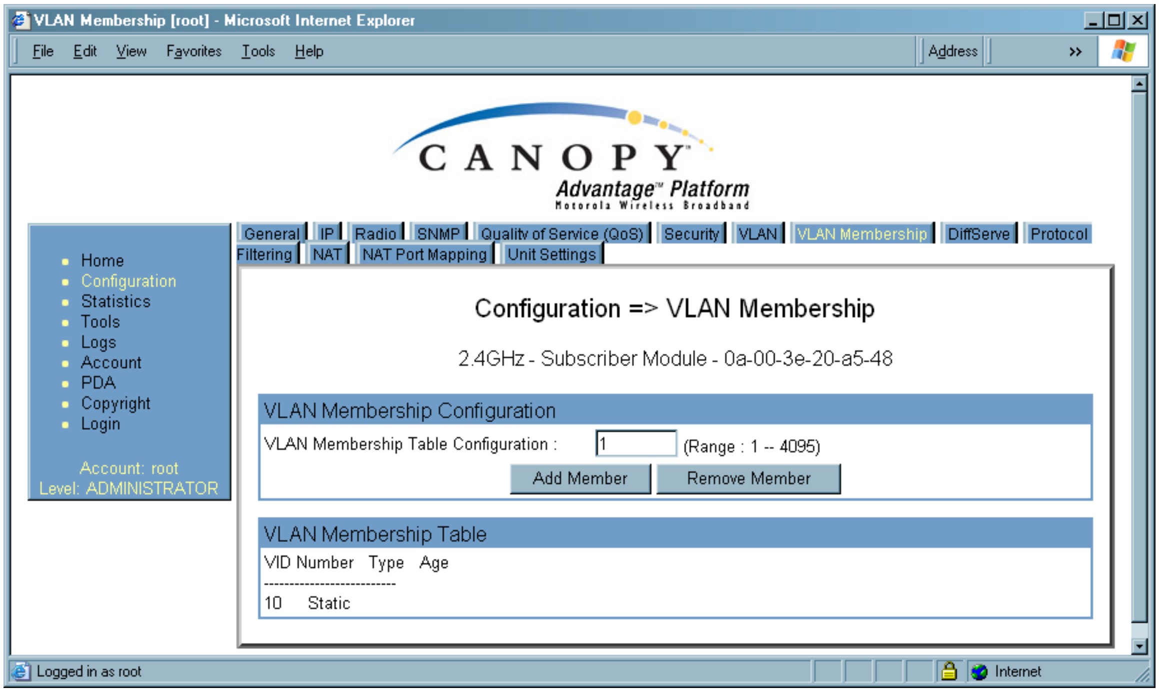
Reboot

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.



Configuration => VLAN Membership

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

VLAN Membership Configuration

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

VLAN Membership Table

```
VID Number   Type   Age
--------------------------
10     Static
```

Figure 95: VLAN Membership tab of SM, example

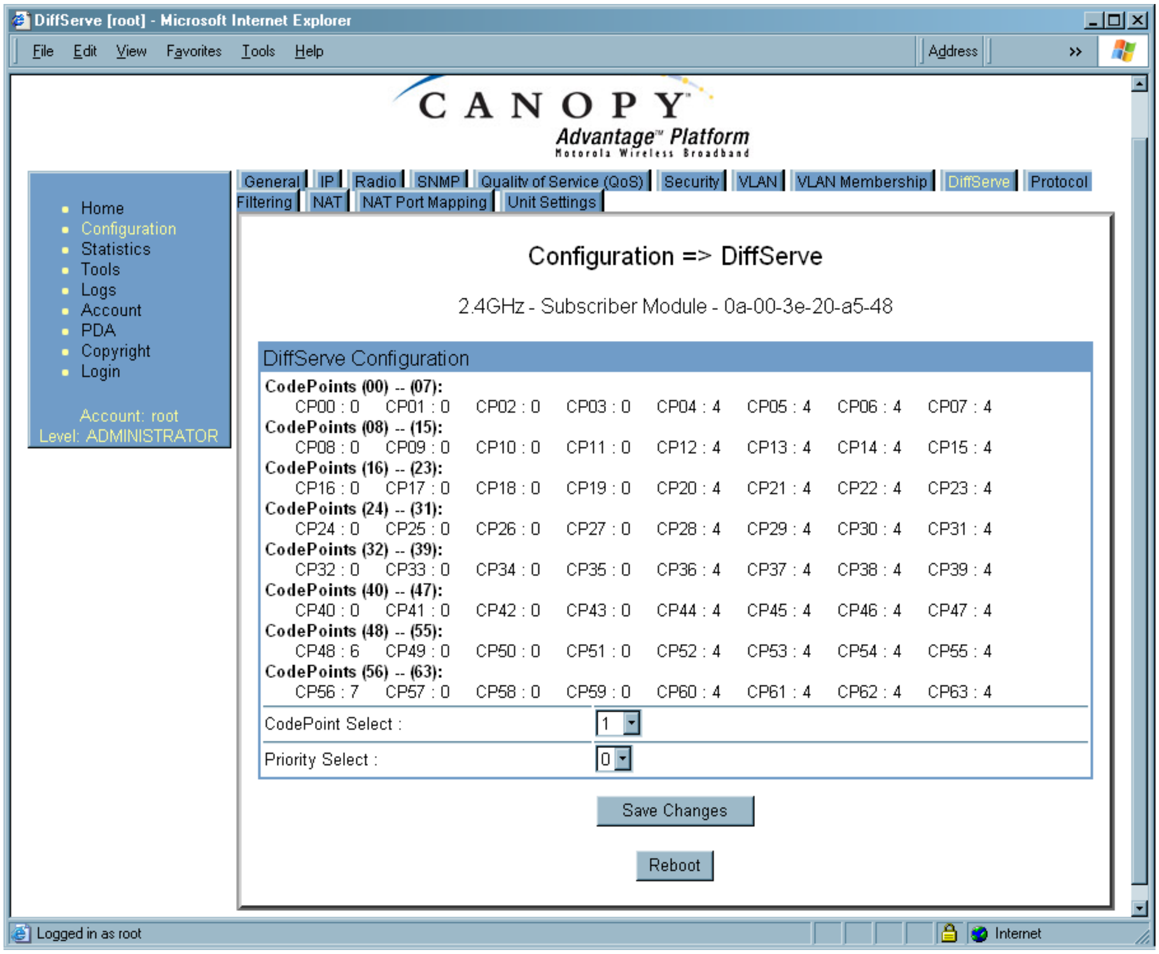
In the VLAN Membership tab, you may set the following parameter.

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.



Configuration => DiffServe

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

DiffServe Configuration

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

CodePoint Select : 1

Priority Select : 0

Figure 96: DiffServe tab of SM, example

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

CodePoint 1 through CodePoint 47

CodePoint 49 through CodePoint 55

CodePoint 57 through CodePoint 63

The default priority value for each settable CodePoint is shown in Figure 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).

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.

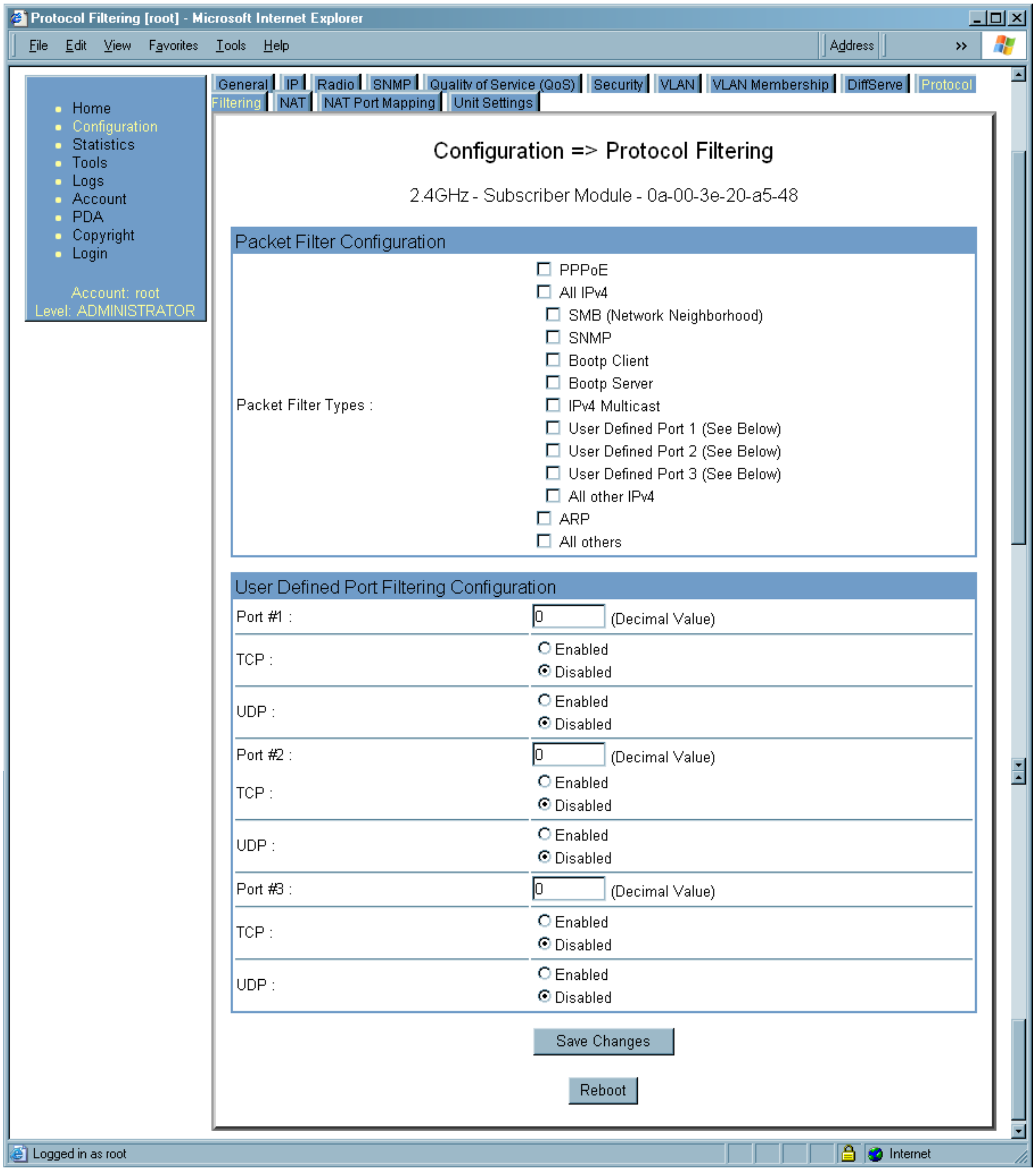
Save Changes
When you click this button, any changes that you made on this tab are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

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.



Configuration => Protocol Filtering

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

Packet Filter Configuration

Packet Filter Types :

- □ PPPoE
- □ All IPv4
  - □ SMB (Network Neighborhood)
  - □ SNMP
  - □ Bootp Client
  - □ Bootp Server
  - □ IPv4 Multicast
  - □ User Defined Port 1 (See Below)
  - □ User Defined Port 2 (See Below)
  - □ User Defined Port 3 (See Below)
  - □ All other IPv4
- □ ARP
- □ All others

User Defined Port Filtering Configuration

Port #1 :	0 (Decimal Value)
TCP :	○ Enabled ● Disabled
UDP :	○ Enabled ● Disabled
Port #2 :	0 (Decimal Value)
TCP :	○ Enabled ● Disabled
UDP :	○ Enabled ● Disabled
Port #3 :	0 (Decimal Value)
TCP :	○ Enabled ● Disabled
UDP :	○ Enabled ● Disabled

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 383.

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

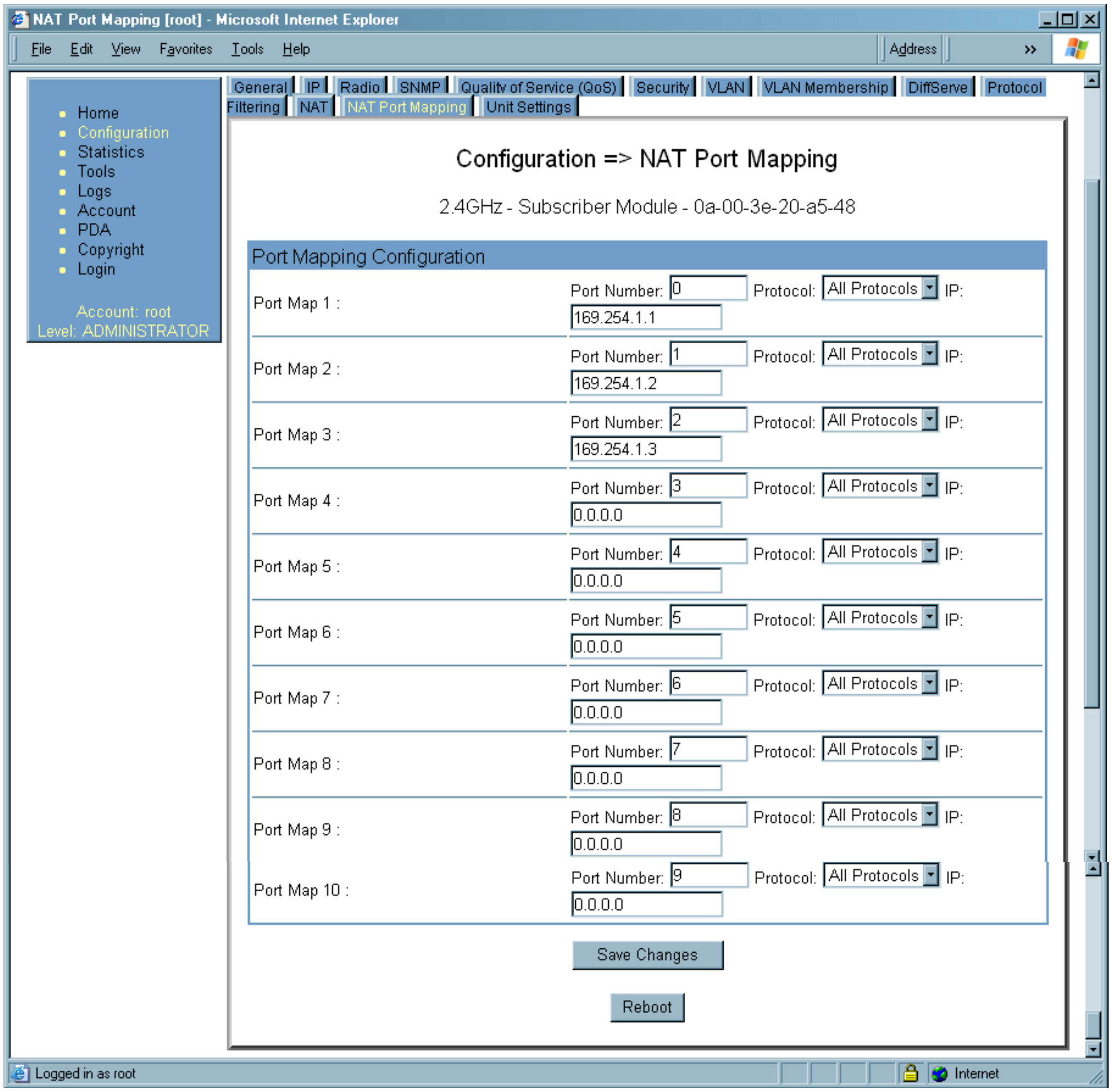
- Check the box for **User Defined Port *n* (See Below)** in the **Packet Filter Types** section of this tab.
- In the **User Defined Port Filtering Configuration** section of this tab, both
  - provide a port number at **Port #*n***.
  - check **TCP**, **UDP**, or both.

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 382.

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.



Configuration => NAT Port Mapping

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

Port Mapping Configuration

Port Map 1 :	Port Number: 0	Protocol: All Protocols	IP: 169.254.1.1
Port Map 2 :	Port Number: 1	Protocol: All Protocols	IP: 169.254.1.2
Port Map 3 :	Port Number: 2	Protocol: All Protocols	IP: 169.254.1.3
Port Map 4 :	Port Number: 3	Protocol: All Protocols	IP: 0.0.0.0
Port Map 5 :	Port Number: 4	Protocol: All Protocols	IP: 0.0.0.0
Port Map 6 :	Port Number: 5	Protocol: All Protocols	IP: 0.0.0.0
Port Map 7 :	Port Number: 6	Protocol: All Protocols	IP: 0.0.0.0
Port Map 8 :	Port Number: 7	Protocol: All Protocols	IP: 0.0.0.0
Port Map 9 :	Port Number: 8	Protocol: All Protocols	IP: 0.0.0.0
Port Map 10 :	Port Number: 9	Protocol: All Protocols	IP: 0.0.0.0

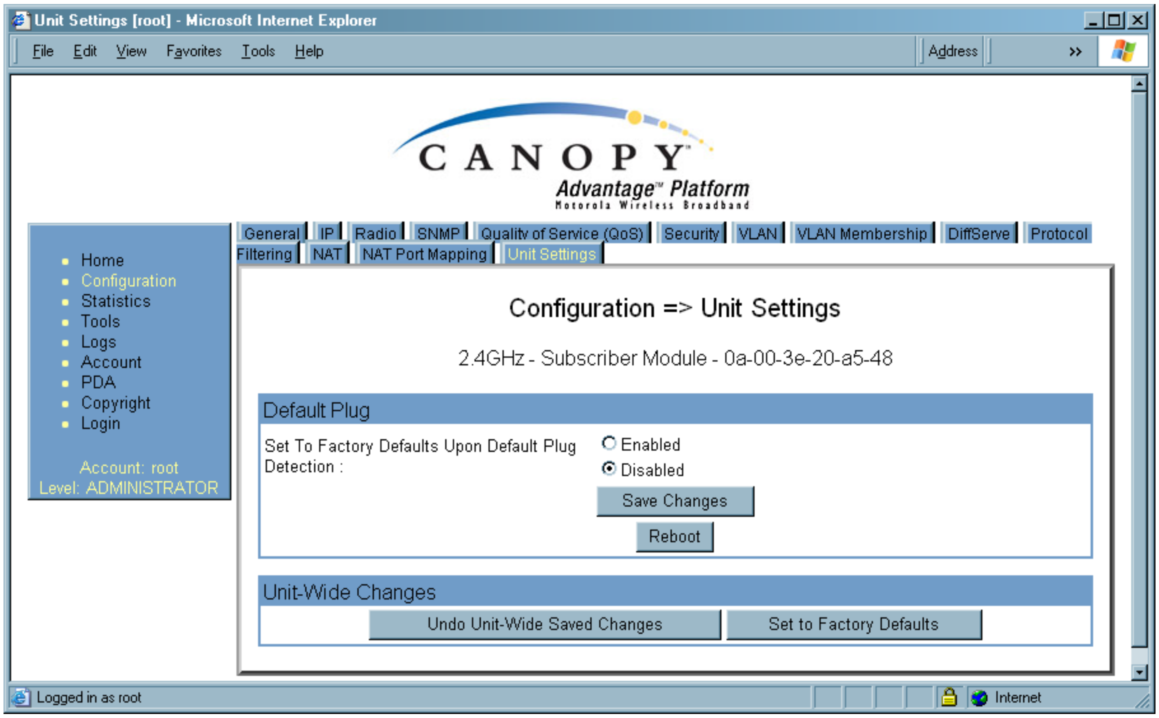
Figure 98: NAT Port Mapping tab of SM, example

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.



Configuration => Unit Settings

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

Default Plug

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

Unit-Wide Changes

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 379.

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	**Authentication Mode**	Configuration> Security	AP	**Authentication Disabled**
	Configuration Source	Configuration> General	AP	**SM**
BAM Release 2.0 (Consider upgrading to Prizm)	**Authentication Mode**	Configuration	AP	**Authentication Required**
	Configuration Source	Configuration	AP	**BAM+SM**
BAM Release 2.1 (Consider upgrading to Prizm)	**Authentication Mode**	Configuration	AP	**Authentication Required**
	Configuration Source	Configuration	AP	**BAM**
Prizm Release 2.0 and 2.1 (being used for BAM functionality)	**Authentication Mode**	Configuration	AP	**Authentication Required**
	Configuration Source	Configuration	AP	**BAM**

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 Cyclone 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.

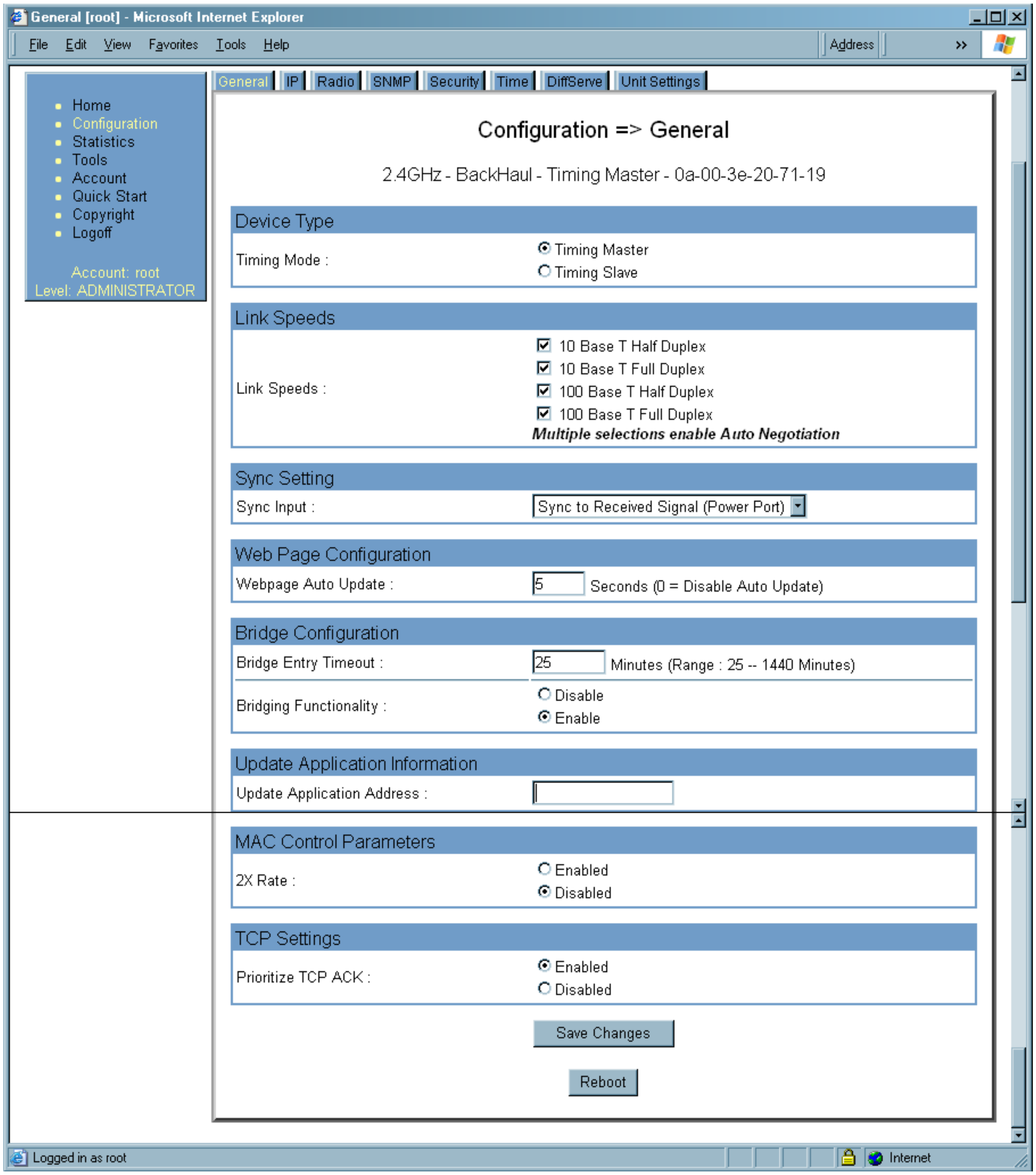
18.4 CONFIGURING A BH TIMING MASTER FOR THE DESTINATION

NOTE:
The PTP 400 and PTP 600 series bridges (previously known as 30/60 Mbps and 150/300 Mbps Backhauls) 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 377.

18.4.1 General Tab of the BHM

An example of the General tab in a BHM is displayed in Figure 100.



Configuration => General

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

Device Type

Timing Mode : ● Timing Master ○ Timing Slave

Link Speeds

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

Sync Setting

Sync Input : Sync to Received Signal (Power Port)

Web Page Configuration

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

Bridge Configuration

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

Bridging Functionality : ○ Disable ● Enable

Update Application Information

Update Application Address :

MAC Control Parameters

2X Rate : ○ Enabled ● Disabled

TCP Settings

Prioritize TCP ACK : ● Enabled ○ Disabled

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 90.

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.