

OPERATIONS GUIDE

21 GROWING YOUR NETWORK

Keys to successfully growing your network include

- monitoring the RF environment.
- considering software release compatibility.
- redeploying modules appropriately and quickly.

21.1 MONITORING THE RF ENVIRONMENT

Regardless of whether you are maintaining or growing your network, you may encounter new RF traffic that can interfere with your current or planned equipment. Regularly measuring *over a period of time* and logging the RF environment, as you did before you installed your first equipment in an area, enables you to recognize and react to changes.

21.1.1 Spectrum Analyzer

IMPORTANT!



The following sections describe the use of a Canopy module in scan mode to analyze the RF spectrum. While a module is in the scan mode, no RF connectivity to that module is possible until either you click **Disable** on the Spectrum Analyzer page or 15 minutes elapses since the module entered the scan mode.

For this reason

- *do not* enable the spectrum analyzer from an RF-connected module. (No readings will be displayed when the RF connection is re-established.)
- be advised that, if you enable the spectrum analyzer by Ethernet connection, any current RF connection to that module drops.

You can use any AP, SM, or BHS to see at once the frequency and power level of any detectable signal that is within, above, or below the frequency band range of the module.



RECOMMENDATION:

Vary the days and times when you analyze the spectrum in an area. The RF environment can change throughout the day or throughout the week.

Temporarily deploy an SM or BHS for *each* frequency band range that you need to monitor and access the Spectrum Analyzer tab in the Tools web page of the module. (For access from a PDA, see [PDA Access to Canopy Modules](#) on Page 331.) To enter the scan mode and view readings, click **Enable**.

21.1.2 Graphical Spectrum Analyzer Display

An SM/BHS displays the graphical spectrum analyzer. An example of the Spectrum Analyzer tab is shown in [Figure 143](#).

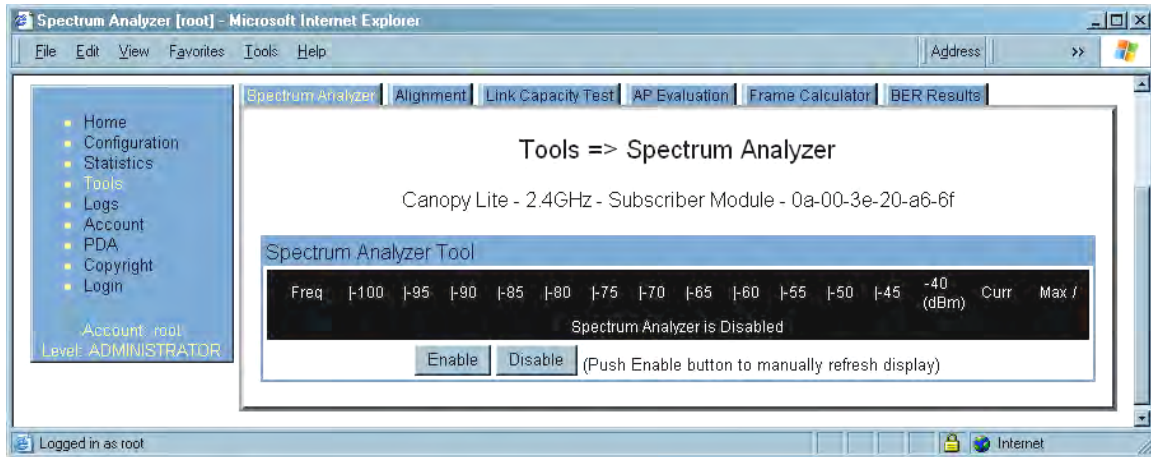


Figure 143: Spectrum Analyzer tab of SM, example

Colors in the display have the following meanings:

- Green bars show the most recent measurements.
- Yellow ticks show the maximum measurements from the current spectrum analysis session.
- Red ticks show measurements of -40 dBm or stronger.

To keep the displayed data current, either set this page to automatically refresh or repeatedly click the **Enable** button. When you are finished analyzing the spectrum, click the **Disable** button to return the module to normal operation.

21.1.3 Using the AP as a Spectrum Analyzer

You can temporarily transform an AP into an SM and thereby use the spectrum analyzer functionality. This is the only purpose supported for the transformation.



CAUTION!

You lose connectivity to the AP during spectrum analysis, have no service to any SMs that are connected to it, and can regain connectivity (and toggle it back to AP) through only the wired Ethernet interface to the AP. For this reason, you should perform the transformation to SM in the *Ethernet* interface.

To transform the AP into an SM for spectrum analysis and then return the device to an AP, perform the following steps.

Procedure 34: Using the Spectrum Analyzer in AP feature

1. Connect to the wired Ethernet interface of the AP.
2. Access the General tab of the Configuration page in the AP.
3. Set the **Device Setting** parameter to **SM**.
4. Click the **Save Changes** button.
5. Click the **Reboot** button.

6. When the module has rebooted as an SM, click the Tools navigation link on the left side of the Home page.
7. Click the Spectrum Analyzer tab.
8. Either set this page to automatically refresh or repeatedly click the **Enable** button.
RESULT: The SM enters the scan mode.
9. When you are finished analyzing the spectrum, click the **Disable** button.
10. In the left-side navigation links, click Configuration.
11. Click the General tab.
12. Set the **Device Setting** parameter to **AP**.
13. Click the **Save Changes** button.
14. Click the **Reboot** button.
RESULT: The AP boots with its previous frequency setting.

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

21.2 CONSIDERING SOFTWARE RELEASE COMPATIBILITY

Within the same Canopy network, modules can operate on multiple software releases. However, the features that can be enabled are limited to those that the earliest software supports.

21.2.1 Designations for Hardware in Radios

Canopy documentation refers to hardware series (for example, Series P9). Canopy Release 8 requires APs, BHs, and AES SMs to be Series P9 or later hardware. The correlation between hardware series and the MAC addresses of the radio modules is provided in [Table 55](#).

Table 55: Hardware series by MAC address

| Radio Frequency Band Range | Hardware Series | |
|----------------------------|---------------------------------|------------------------------------|
| | P7 or P8 in These MAC Addresses | P9 or Later in These MAC Addresses |
| 900 | None | All |
| 2.4 | ≤ 0A003E20672B | ≥ 0A003E20672C |
| 5.2 | ≤ 0A003E00F4E3 | ≥ 0A003E00F4E4 |
| 5.4 | None | All |
| 5.7 | ≤ 0A003EF12AFE | ≥ 0A003EF12AFF |

Differences in capabilities among these hardware series are summarized in [Table 56](#).

Table 56: Hardware series differences

| Capability | Availability per Hardware Series | | |
|----------------------------------|----------------------------------|-----|-----|
| | P7 | P8 | P9 |
| Auto-sense Ethernet cable scheme | no | yes | yes |

| | | | |
|---|----|-----|-----|
| Support CMMmicro | no | yes | yes |
| Support hardware scheduling in APs ¹ | no | no | yes |
| Support 2X operation in APs and SMs | no | no | yes |
| NOTES: | | | |
| 1. An SM of P7 or P8 series requires an FPGA load through CNUF for access to hardware scheduling, and then only at 1X operation. An AP of P7 or P8 series cannot perform hardware scheduling. | | | |

Advantage Series P9 APs provide higher throughput and lower latency than earlier series Advantage APs and support configuring the high-priority channel per SM. Regular Canopy Series P9 APs *do not* provide the higher throughput and lower latency, but they do support configuring the high-priority channel per SM.

21.2.2 CMMmicro Software and Hardware Compatibility

The CMMmicro contains both a programmable logic device (PLD) and software. These must be compatible. For example, the PLD that is compatible with CMMmicro Release 2.0.8 is PLD 5. Further, the CMMmicro must be compatible with both the application software release and the hardware of attached APs and BHs. These attached modules must have been manufactured in October 2002 or later.

APs and BHs that were manufactured earlier do not support sync on the power leads of the Ethernet port. To determine whether the AP or BH hardware is compatible with the CMMmicro, see [Table 57](#).

Table 57: AP/BH compatibility with CMMmicro

| Frequency Band Range | Range of MAC Addresses (ESNs) | |
|----------------------|-------------------------------|--------------------------|
| | Incompatible with CMMmicro | Compatible with CMMmicro |
| 900 MHz AP | none | all |
| 2.4 GHz | none | all |
| 5.2 GHz | ≤ 0A003E0021C8 | ≥ 0A003E0021C9 |
| 5.4 GHz | none | all |
| 5.7 GHz | ≤ 0A003EF00F79 | ≥ 0A003EF00F7A |

21.2.3 MIB File Set Compatibility

Although MIB files are text files (not software), they define objects associated with configurable parameters and indicators for the module and its links. In each release, some of these parameters and indicators are not carried forward from the previous release, and some parameters and indicators are introduced or changed.

For this reason, use the MIB files from your download to replace previous MIB files in conjunction with your software upgrades, even if the file names are identical to those of your previous files. Date stamps on the MIB files distinguish the later set.

21.3 REDEPLOYING MODULES

Successfully redeploying a module may involve

- maintaining full and accurate records of modules being redeployed from warehouse stock.
- exercising caution about
 - software compatibility. For example, whether desired features can be enabled with the redeployed module in the network.
 - procedural handling of the module. For example
 - whether to align the SM or BHS by power level and jitter or by only jitter.
 - whether the module auto-senses the Ethernet cable connector scheme.
 - hardware compatibility. For example, where a CMMmicro is deployed.
 - the value of each configurable parameter. Whether all are compatible in the new destination.
- remembering to use auto discovery to add the redeployed SM to the network in Prizm.

21.3.1 Wiring to Extend Network Sync

The following procedure can be used to extend network sync by one additional hop, as described under [Passing Sync in an Additional Hop](#) on Page 97. Where a collocated module receives sync over the air, the collocated modules can be wired to pass the sync as follows:

Procedure 35: Extending network sync

1. Connect the GPS Utility ports of the collocated modules using a sync cable with RJ-11 connectors.
2. Set the **Sync Input** parameter on the Configuration page of the collocated AP or BH timing master to **Sync to Received Signal (Timing Port)**.
3. Set the **Frame Timing Pulse Gated** parameter on the Configuration page of the collocated SM or BH timing slave to **Enable**.
NOTE: This setting prevents interference in the event that the SM or BH timing slave loses sync.

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

22 SECURING YOUR NETWORK

22.1 ISOLATING APs FROM THE INTERNET

Ensure that the IP addresses of the APs in your network

- are not routable over the Internet.
- do not share the subnet of the IP address of your user.

RFC 1918, *Address Allocation for Private Subnets*, reserves for private IP networks three blocks of IP addresses that are not routable over the Internet:

- /8 subnets have one reserved network, 10.0.0.0 to 10.255.255.255.
- /16 subnets have 16 reserved networks, 172.16.0.0 to 172.31.255.255.
- /24 subnets have 256 reserved networks, 192.168.0.0 to 192.168.255.255.

22.2 ENCRYPTING CANOPY RADIO TRANSMISSIONS

Canopy systems employ the following forms of encryption for security of the wireless link:

- BRAID—a security scheme that the cellular industry uses to authenticate wireless devices.
- DES—Data Encryption Standard, an over-the-air link option that uses secret 56-bit keys and 8 parity bits.
- AES—Advanced Encryption Standard, an extra-cost over-the-air link option that provides extremely secure wireless connections. AES uses 128-bit secret keys as directed by the government of the U.S.A. AES is not exportable and requires a special AP to process the large keys.

BRAID is a stream cipher that the TIA (Telecommunications Industry Association) has standardized. Standard Canopy APs and SMs use BRAID encryption to

- calculate the per-session encryption key (independently) on each end of a link.
- provide the digital signature for authentication challenges.

22.2.1 DES Encryption

Standard Canopy modules provide DES encryption. DES performs a series of bit permutations, substitutions, and recombination operations on blocks of data. DES Encryption does not affect the performance or throughput of the system.

22.2.2 AES Encryption

Motorola also offers Canopy products that provide AES encryption. AES uses the Rijndael algorithm and 128-bit keys to establish a higher level of security than DES. Because of this higher level of security, the government of the U.S.A. controls the export of communications products that use AES (among which the Canopy AES feature activation key is one) to ensure that these products are available in only certain regions and by special permit.

The Canopy distributor or reseller can advise service providers about current regional availability. Canopy AES products are certified as compliant with the Federal Information Processing Standards (FIPS) in the U.S.A. The National Institute of Standards and Technology (NIST) in the U.S.A. has specified AES for significantly greater security than that which DES provides. NIST selected the AES algorithm for providing the best combination of security, performance, efficiency, implementation, and flexibility. NIST collaborates with industry to develop and apply technology, measurements, and standards.

22.2.3 AES-DES Operability Comparisons

This section describes the similarities and differences between DES and AES products, and the extent to which they may interoperate.

The DES AP and the DES BHM modules are factory-programmed to enable or disable *DES* encryption. Similarly, the AES AP and the AES BHM modules are factory-programmed to enable or disable *AES* encryption. In either case, the authentication key entered in the Configuration page establishes the encryption key. For this reason, the authentication key must be the same on each end of the link. See [Authentication Key](#) on Page 283.

Feature Availability

Canopy AES products run the same software as DES products. Thus feature availability and functionality are and will continue to be the same, regardless of whether AES encryption is enabled. All interface screens are identical. However, when encryption is enabled on the Configuration screen

- the AES product provides AES encryption.
- the DES product provides DES encryption.

Canopy AES products and DES products use different FPGA (field-programmable gate array) loads. However, the AES FPGA will be upgraded as needed to provide new features or services similar to those available for DES products.

Canopy DES products cannot be upgraded to AES. To have the option of AES encryption, the operator must purchase AES products.

Interoperability

Canopy AES products and DES products do not interoperate when enabled for encryption. For example, An AES AP with encryption enabled cannot communicate with DES SMs. Similarly, an AES Backhaul timing master module with encryption enabled cannot communicate with a DES Backhaul timing slave module.

However, if encryption is disabled, AES modules can communicate with DES modules.

22.3 MANAGING MODULE ACCESS BY PASSWORDS

22.3.1 Adding a User for Access to a Module

From the factory, each Canopy module has a preconfigured administrator-level account in the name `root`, which initially requires no associated password. This is the same `root` account that you may have used for access to the module by `telnet` or `ftp`. If you upgrade a module to Release 8

- an account is created in the name `admin`.
- both `admin` and `root` inherit the password that was previously used for access to the module:
 - the **Full Access** password, if one was set.
 - the **Display-Only Access** password, if one was set and no Full Access password was set.



IMPORTANT!

If you use Prizm, *do not* delete the `root` account from any module. If you use an NMS that communicates with modules through SNMP, *do not* delete the `root` account from any module unless you first can confirm that the NMS does not rely on the `root` account for access to the modules.

Each module supports four or fewer user accounts, regardless of account levels. The available levels are

- **ADMINISTRATOR**, who has full read and write permissions. This is the level of the `root` and `admin` users, as well as any other administrator accounts that one of them creates.
- **INSTALLER**, who has permissions identical to those of **ADMINISTRATOR** except that the installer cannot add or delete users or change the password of any other user.
- **GUEST**, who has no write permissions and only a limited view of General Status tab, as shown in [Figure 144](#), and can log in as a user.

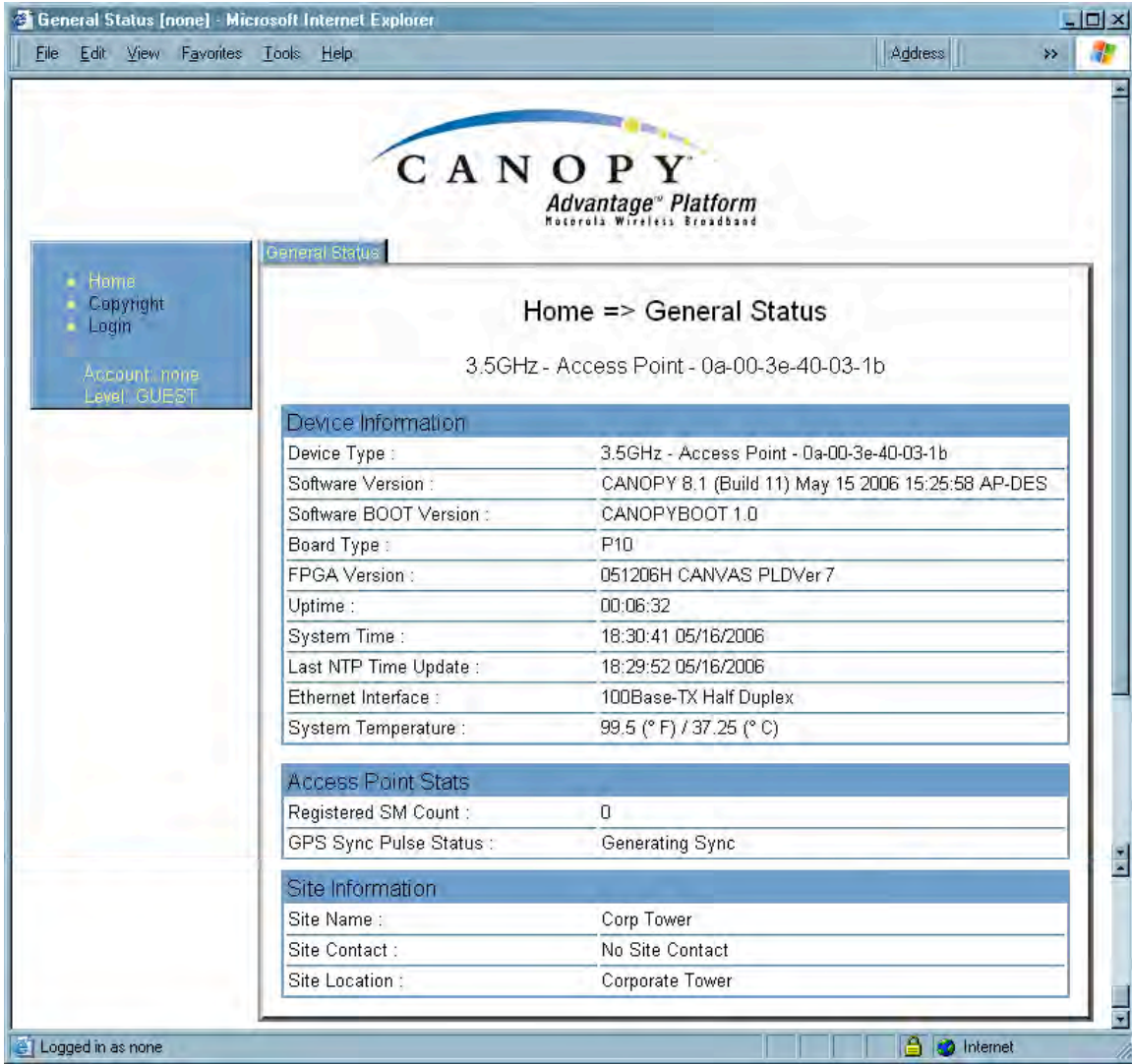


Figure 144: General Status tab view for GUEST-level account

An example of the Add User tab is displayed in [Figure 145](#).

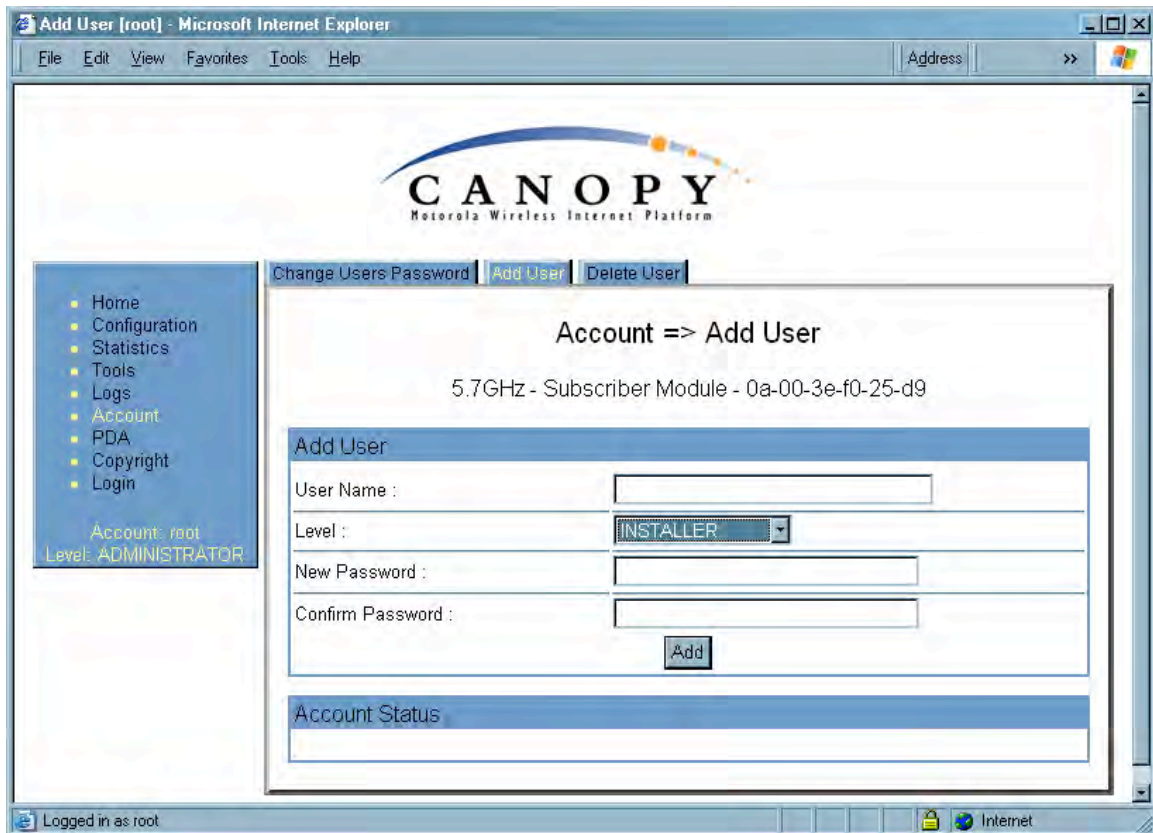


Figure 145: Add User tab of SM, example

After a password has been set for any ADMINISTRATOR-level account, initial access to the module GUI opens the view of GUEST level (Figure 144).

Accounts that cannot be deleted are

- the current user's own account.
- the last remaining account of ADMINISTRATOR level.

22.3.2 Overriding Forgotten IP Addresses or Passwords on AP, SM, or BH

Canopy systems offer a plug that allows you to temporarily override some AP/SM/BH settings and thereby regain control of the module. This plug is needed for access to the module in any of the following cases:

- You have forgotten either
 - the IP address assigned to the module.
 - the password that provides access to the module.
- The module has been locked by the No Remote Access feature. (See [Denying All Remote Access](#) on Page 453 and [Reinstating Remote Access Capability](#) on Page 453.)
- You want local access to a module that has had the 802.3 link disabled in the Configuration page.

You can configure the module such that, when it senses the override plug, it responds by either

- resetting the LAN1 IP address to 169.254.1.1, allowing access through the default configuration without *changing* the configuration, whereupon you will be able to view and reset any non-default values as you wish.
- resetting all configurable parameters to their factory default values.

Acquiring the Override Plug

You can either purchase or fabricate an override plug as follows. To purchase an override plug for a nominal fee, order the plug at <http://www.best-tronics.com/motorola.htm>. To fabricate an override plug, perform the following steps.

Procedure 36: Fabricating an override plug

1. Install an RJ-11 6-pin connector onto a 6-inch length of CAT 5 cable.
2. Pin out all 6-pins.
3. Short (solder together) Pins 4 and 6 on the other end. Do not connect any other wires to anything. The result should be as shown in [Figure 146](#).

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

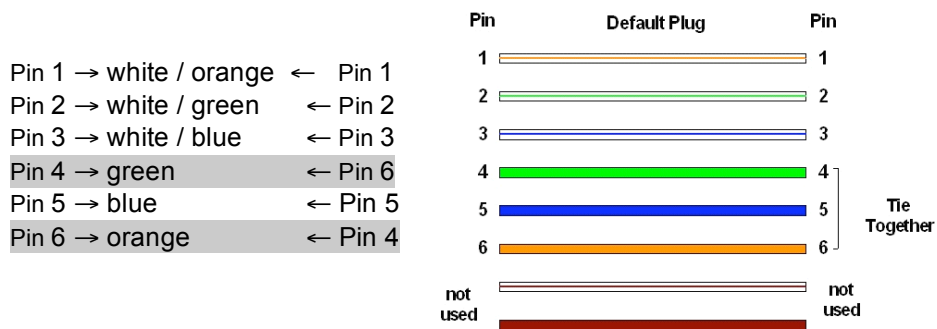



Figure 146: RJ-11 pinout for the override plug

Using the Override Plug



IMPORTANT!

While the override plug is connected to a module, the module can neither register nor allow registration of another module.

To regain access to the module, perform the following steps.

Procedure 37: Regaining access to a module

1. Insert the override plug into the RJ-11 GPS utility port of the module.
2. Power cycle by removing, then re-inserting, the Ethernet cable.
RESULT: The module boots with the default IP address of 169.254.1.1, password fields blank, and all other configuration values as previously set.
3. Wait approximately 30 seconds for the boot to complete.

4. Remove the override plug.
5. Set passwords and IP address as desired.
6. Change configuration values if desired.
7. Click the **Save Changes** button.
8. Click the **Reboot** button.

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


22.3.3 Overriding Forgotten IP Addresses or Passwords on CMMmicro

By using an override toggle switch on the CMMmicro circuit board, you can temporarily override a lost or unknown IP address or password as follows:

- Up is the override position in which a power cycle causes the CMMmicro to boot with the default IP address (169.254.1.1) and no password required.
- Down is the normal position in which a power cycle causes the CMMmicro to boot with your operator-set IP address and password(s).

To override a lost or unknown IP address or password, perform the following steps.

Procedure 38: Using the override switch to regain access to CMMmicro



IMPORTANT!
In override mode

- a CMMmicro provides no power on its ports.
- any APs or BHs connected to the CMMmicro are not powered.
- you cannot gain browser access to the CMMmicro through any connected APs or BHs.

1. Gain physical access to the inside of the CMMmicro enclosure.
2. Establish direct Ethernet connectivity to the CMMmicro (not through an AP or BH).
3. Flip the toggle switch up (toward you).
4. Power cycle the CMMmicro.
RESULT: The module reboots with the default IP address of 169.254.1.1, password fields blank, and all other configuration values as previously set.
5. Set passwords as desired, or enter a blank space to set no password.
6. Change configuration values if desired.
7. Click the **Save Changes** button.
8. Flip the toggle switch down (away from you).
9. Click the **Reboot** button.

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

22.4 REQUIRING SM AUTHENTICATION

Through the use of Prizm Release 2.0 or later, or BAM Release 2.1, you can enhance network security by requiring SMs to authenticate when they register. Three keys and a random number are involved in authentication as follows:

- factory-set key in each SM. Neither the subscriber nor the network operator can view or change this key.
- authentication key, also known as authorization key and skey. This key matches in the SM and AP as the **Authentication Key** parameter, and in the Prizm database.
- random number, generated by Prizm or BAM and used in each attempt by an SM to register and authenticate. The network operator can view this number.
- session key, calculated separately by the SM and Prizm or BAM, based on both the authentication key (or, by default, the factory-set key) and the random number. Prizm or BAM sends the session key to the AP. The network operator cannot view this key.

None of the above keys is ever sent in an over-the-air link during an SM registration attempt. However, with the assumed security risk, the operator can create and configure the **Authentication Key** parameter. See [Authentication Key](#) on Page 283.

22.5 FILTERING PROTOCOLS AND PORTS

You can filter (block) specified protocols and ports from leaving the SM and entering the Canopy network. This protects the network from both intended and inadvertent packet loading or probing by network users. By keeping the specified protocols or ports off the network, this feature also provides a level of protection to users from each other.

Protocol and port filtering is set per SM. Except for filtering of SNMP ports, filtering occurs as packets leave the SM. If an SM is configured to filter SNMP, then SNMP packets are blocked from entering the SM and, thereby, from interacting with the SNMP portion of the protocol stack on the SM.

22.5.1 Port Filtering with NAT Enabled

Where NAT is enabled, you can filter only the three user-defined ports. The following are example situations in which you can configure port filtering where NAT is enabled.

- To block a subscriber from using FTP, you can filter Ports 20 and 21 (the FTP ports) for both the TCP and UDP protocols.
- To block a subscriber from access to SNMP, you can filter Ports 161 and 162 (the SNMP ports) for both the TCP and UDP protocols.
NOTE: In only the SNMP case, filtering occurs before the packet interacts with the protocol stack.

22.5.2 Protocol and Port Filtering with NAT Disabled

Where NAT is disabled, you can filter both protocols and the three user-defined ports. Using the check boxes on the interface, you can either

- allow all protocols except those that you wish to block.
- block all protocols except those that you wish to allow.

You can allow or block any of the following protocols:

- PPPoE (Point to Point Protocol over Ethernet)
- Any or all of the following IPv4 (Internet Protocol version 4) protocols:
 - SMB (Network Neighborhood)
 - SNMP

- Up to 3 user-defined ports
- All other IPv4 traffic (see [Figure 147](#))
- Uplink Broadcast
- ARP (Address Resolution Protocol)
- All others (see [Figure 147](#))

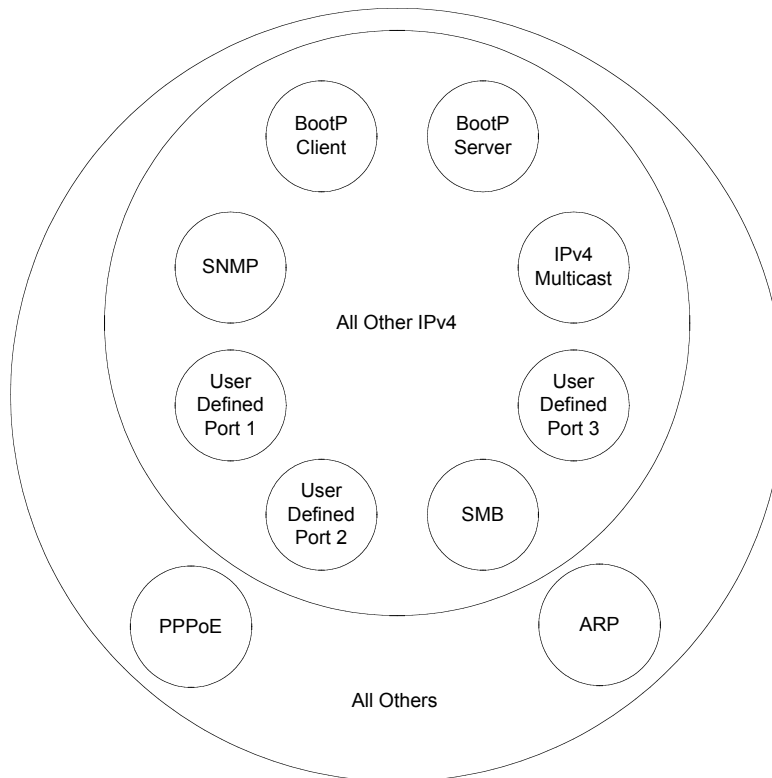


Figure 147: Categorical protocol filtering

The following are example situations in which you can configure protocol filtering where NAT is disabled:

- If you block a subscriber from only PPOE and SNMP, then the subscriber retains access to all other protocols and all ports.
- If you block PPOE, IPv4, and Uplink Broadcast, and you also check the **All others** selection, then only Address Resolution Protocol is not filtered.

The ports that are filtered as a result of protocol selections in the Protocol Filtering tab of the SM are listed in [Table 58](#). Further information is provided under [Protocol Filtering Tab of the SM](#) on Page [289](#).

Table 58: Ports filtered per protocol selections

| Protocol Selected | Port Filtered (Blocked) |
|-------------------|--|
| SMB | Destination Ports 137 TCP and UDP, 138 UDP, 139 TCP, 445 TCP |
| SNMP | Destination Ports 161 TCP and UDP, 162 TCP and UDP |
| Bootp Client | Source Port 68 UDP |
| Bootp Server | Source Port 67 UDP |

22.6 ENCRYPTING DOWNLINK BROADCASTS

An AP can be enabled to encrypt downlink broadcast packets such as the following:

- ARP
- NetBIOS
- broadcast packets containing video data on UDP.

The encryption used is DES for a DES module, and AES for an AES module. Before the Encrypt Downlink Broadcast feature is enabled on the AP, air link security should be enabled on the AP.

22.7 ISOLATING SMs

In the Release 8 or later AP, you can prevent SMs in the sector from directly communicating with each other. In CMMmicro Release 2.2 or later, you can prevent connected APs from directly communicating with each other, which prevents SMs that are in different sectors of a cluster from communicating with each other.

In the AP, the **SM Isolation** parameter is available in the General tab of the Configuration web page. In the drop-down menu for that parameter, you can configure the SM Isolation feature by any of the following selections:

- **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.

In the CMMmicro, SM isolation treatment is the result of how you choose to manage the port-based VLAN feature of the embedded switch, where you can switch all traffic from any AP or BH to an uplink port that you specify. However, this is not packet level switching. It is not based on VLAN IDs. See the **VLAN Port Configuration** parameter in [Figure 78: Configuration page of CMMmicro, example](#) on Page 224.

22.8 FILTERING MANAGEMENT THROUGH ETHERNET

You can configure the SM to disallow any device that is connected to its Ethernet port from accessing the IP address of the SM. If you set the **Ethernet Access Control** parameter to **Enabled**, then

- no attempt to access the SM management interface (by http, SNMP, telnet, ftp, or tftp) through Ethernet can succeed.
- any attempt to access the SM management interface over the air (by IP address, presuming that **LAN1 Network Interface Configuration, Network Accessibility** is set to **Public**, or by link from the Session Status or Remote Subscribers tab in the AP) is unaffected.

22.9 ALLOWING MANAGEMENT FROM ONLY SPECIFIED IP ADDRESSES

The Security tab of the Configuration web page in the AP, SM, and BH includes the **IP Access Control** parameter. You can specify one, two, or three IP addresses that should be allowed to access the management interface (by http, SNMP, telnet, ftp, or tftp).

If you select

- **IP Access Filtering Disabled**, then management access is allowed from any IP address, even if the **Allowed Source IP 1 to 3** parameters are populated.
- **IP Access Filtering Enabled**, and specify at least one address in the **Allowed Source IP 1 to 3** parameter, then management access is limited to the specified address(es). If you intend to use Prizm to manage the element, then you must ensure that the IP address of the Prizm server is listed here.

22.10 CONFIGURING MANAGEMENT IP BY DHCP

The IP tab in the Configuration web page of every Canopy radio contains a **LAN1 Network Interface Configuration, DHCP State** parameter that, if enabled, causes the IP configuration (IP address, subnet mask, and gateway IP address) to be obtained through DHCP instead of the values of those individual parameters. The setting of this DHCP state parameter is also viewable, but not settable, in the Network Interface tab of the Home page.

In the SM, this parameter is settable

- in the NAT tab of the Configuration web page, but only if NAT is enabled.
- in the IP tab of the Configuration web page, but only if the **Network Accessibility** parameter in the IP tab is set to **Public**.

23 MANAGING BANDWIDTH AND AUTHENTICATION

This section provides a high-level description of bandwidth and authentication management in a Canopy network. For more specific information, see *Canopy Bandwidth and Authentication Manager (BAM) User Guide* or the *Motorola Canopy Prizm User Guide*.

23.1 MANAGING BANDWIDTH WITHOUT BAM

Unless Prizm or BAM is deployed and is configured in the AP, bandwidth management is limited to applying a single sustained data rate value (for uplink and for downlink) and a single burst allocation value (for uplink and for downlink) to every SM that registers in the AP.

23.2 BANDWIDTH AND AUTHENTICATION MANAGER (BAM) SERVICES AND FEATURES

Prizm or BAM enables you to perform the following management operations on SMs:

- Change the key that the SMs need for authenticating.
- Temporarily suspend or reinstate a subscriber.
- Set burst size and data transfer rate caps for an SM or group of SMs.
- Use licensing to uncap an SM or group of SMs.
- List all ESNs that are associated with a specified VLAN ID.
- Associate or dissociate an SM or group of SMs with a specified VLAN ID.
- Set VLAN parameters.
- Toggle whether to send those VLAN parameters to the SMs.
- Set CIR parameters for low-priority and high-priority channel rates.
- Toggle whether to send those CIR parameters to the SMs.
- Toggle whether to enable the high-priority channel in the SMs.

23.2.1 Bandwidth Manager Capability

Prizm or BAM allows you to set bandwidth per SM for sustained rates and burst rates. With this capability, the Canopy system allows both

- burst rates beyond those of many other broadband access solutions.
- control of average bandwidth allocation to prevent excessive bandwidth usage by a subscriber.

All packet throttling occurs in the SMs and APs based on Quality of Service (QoS) data that the Prizm or BAM server provides. No server processing power or network messages are needed for packet throttling.

QoS management also supports marketing of broadband connections at various data rates, for operator-defined groups of subscribers, and at various price points. This allows you to meet customer needs at a price that the customer deems reasonable and affordable.

When BAM is enabled in the AP Configuration page, bandwidth management is expanded to apply uniquely specified sustained data rate and burst allocation values to each registered SM. Thus, you can define differently priced tiers of subscriber service.

Designing Tiered Subscriber Service Levels

Examples of levels of service that vary by bandwidth capability are provided in [Table 59](#) and [Table 60](#).



NOTE:

The speeds that these tables correlate to service levels are comparative examples. Actual download times may be greater due to use of the bandwidth by other SMs, congestion on the local network, congestion on the Internet, capacity of the serving computer, or other network limitations.

Table 59: Example times to download for arbitrary tiers of service with Canopy AP

| Equipment | AP | Canopy | | |
|------------------|---------------------------------------|-----------|-----------|----------|
| | SM | Canopy | | |
| | Operation | 1X | | |
| | Max burst speed | 4.4 Mbps | | |
| Example Settings | Service Type | Premium | Regular | Basic |
| | Sustained Downlink Data Rate | 5250 Kbps | 1000 Kbps | 256 Kbps |
| | Sustained Uplink Data Rate | 1750 Kbps | 500 Kbps | 128 Kbps |
| | Downlink and Uplink Burst Allocations | 500000 Kb | 80000 Kb | 40000 Kb |
| Download (sec) | Web page | <1 | <1 | <1 |
| | 5 MB | 9 | 9 | 9 |
| | 20 MB | 36 | 80 | 470 |
| | 50 MB | 91 | 320 | 1400 |
| | 300 MB | 545 | 2320 | 9220 |

Table 60: Example times to download for arbitrary tiers of service with Advantage AP

| Equipment | AP | Advantage | | | | | | Advantage |
|------------------|---------------------------------------|-----------|-----------|----------|-----------|-----------|----------|------------|
| | SM | Canopy | | | | | | Advantage |
| | Operation | 1X | | | 2X | | | 2X |
| | Max burst speed | 5 Mbps | | | 10 Mbps | | | 10 Mbps |
| Example Settings | Service Type | Premium | Regular | Basic | Premium | Regular | Basic | Premium |
| | Sustained Downlink Data Rate | 5250 Kbps | 1000 Kbps | 256 Kbps | 5250 Kbps | 1000 Kbps | 256 Kbps | 2000 Kbps |
| | Sustained Uplink Data Rate | 1750 Kbps | 500 Kbps | 128 Kbps | 1750 Kbps | 500 Kbps | 128 Kbps | 20000 Kbps |
| | Downlink and Uplink Burst Allocations | 500000 Kb | 80000 Kb | 40000 Kb | 500000 Kb | 80000 Kb | 40000 Kb | 500000 Kb |
| Download (sec) | Web page | <1 | <1 | <1 | <1 | <1 | <1 | <1 |
| | 5 MB | 8 | 8 | 8 | 4 | 4 | 4 | 4 |
| | 20 MB | 32 | 80 | 470 | 16 | 80 | 470 | 16 |
| | 50 MB | 80 | 320 | 1400 | 40 | 320 | 1400 | 40 |
| | 300 MB | 480 | 2320 | 9220 | 362 | 2320 | 9220 | 240 |

23.2.2 Authentication Manager Capability

Prizm or BAM allows you to set per AP a requirement that each SM registering to the AP must authenticate. When AP Authentication Server (APAS) is enabled in the AP, any SM that attempts to register to the AP is denied service if authentication fails, such as (but not limited to) when no Prizm or BAM server is operating or when the SM is not listed in the database.

If a Prizm or BAM server drops out of service where no redundant server exists

- an SM that attempts to register is denied service.
- an SM that is already in session remains in session

In a typical Canopy network, some SMs re-register daily (when subscribers power down the SMs, for example), and others do not re-register in a period of several weeks. Whenever an authentication attempt fails, the SM locks out of any other attempt to register itself to the same AP for the next 15 minutes.

24 MANAGING THE NETWORK FROM A MANAGEMENT STATION (NMS)

SNMPv2 (Simple Network Management Protocol Version 2) can be used to manage and monitor the Canopy modules under SMI (Structure of Management Information) specifications. SMI specifies management information definitions in ASN.1 (Abstract Syntax Notation One) language. SNMPv2 supports both 32-bit and 64-bit counters. The SMI for SNMPv2 is defined in RFC 1902 at <http://www.fags.org/rfc/rfc1902.html>.

24.1 ROLES OF HARDWARE AND SOFTWARE ELEMENTS

24.1.1 Role of the Agent

In SNMP, software on each managed device acts as the *agent*. The agent collects and stores management information in ASN.1 format, in a structure that a MIB (management information base) defines. The agent responds to commands to

- send information about the managed device.
- modify specific data on the managed device.

24.1.2 Role of the Managed Device

In SNMP, the managed device is the network element that operates on the agent software. In the Canopy network, this managed device is the module (AP, SM, or BH). With the agent software, the managed device has the role of server in the context of network management.

24.1.3 Role of the NMS

In SNMP, the NMS (network management station) has the role of client. An application (manager software) operates on the NMS to manage and monitor the modules in the network through interface with the agents.

24.1.4 Dual Roles for the NMS

The NMS can simultaneously act as an agent. In such an implementation, the NMS acts as

- client to the agents in the modules, when polling for the agents for information and sending modification data to the agents.
- server to another NMS, when being polled for information gathered from the agents and receiving modification data to send to the agents.

24.1.5 Simple Network Management Protocol (SNMP) Commands

To manage a module, SNMPv2 supports the `set` command, which instructs the agent to change the data that manages the module.

To monitor a network element (Canopy module), SNMPv2 supports

- the `get` command, which instructs the agent to send information about the module to the manager in the NMS.
- traversal operations, which the manager uses to identify supported objects and to format information about those objects into relational tables.

In a typical Canopy network, the manager issues these commands to the agents of more than one module (to all SMs in the operator network, for example).

24.1.6 Traps from the Agent

When a specified event occurs in the module, the agent initiates a trap, for which the agent sends an unsolicited asynchronous message to the manager.

24.1.7 AP SNMP Proxy to SMs

When the AP receives from Prizm or an NMS an SNMP request for an SM, it is capable of sending that request via proxy to the SM. In this case, the SM responds directly to Prizm or the NMS. (The AP performs no processing on the response.)

24.2 MANAGEMENT INFORMATION BASE (MIB)

The MIB, the SNMP-defined data structure, is a tree of standard branches that lead to optional, non-standard positions in the data hierarchy. The MIB contains both

- objects that SNMP is allowed to control (bandwidth allocation or access, for example)
- objects that SNMP is allowed to monitor (packet transfer, bit rate, and error data, for example).

The path to each object in the MIB is unique to the object. The endpoint of the path is the object identifier.

24.2.1 Cascading Path to the MIB

The standard MIB hierarchy includes the following cascading branch structures:

- the top (standard body) level:
 - ccitt (0)
 - **iso (1)**
 - iso-ccitt (2)
- under iso (1) above:
 - standard (0)
 - registration-authority (1)
 - member-body (2)
 - **identified-organization (3)**
- under identified-organization (3) above:
 - dod (6)
 - other branches
- under dod (6) above:

- internet (1)
- other branches
- o under internet (1) above:
 - mgmt (2)
 - private (4)
 - other branches
- o under mgmt (2) above: **mib-2 (1)** and other branches. (See MIB-II below.)
- o under private (4) above: **enterprise (1)** and other branches. (See Canopy Enterprise MIB below.)

Beneath this level are non-standard branches that the enterprise may define.

Thus, the path to an object that is managed under MIB-II begins with the decimal string **1.3.6.1.2.1** and ends with the object identifier and instance(s), and the path to an object that is managed under the Canopy Enterprise MIB begins with **1.3.6.1.4.1**, and ends with the object identifier and instance(s).

24.2.2 Object Instances

An object in the MIB can have either only a single instance or multiple instances, as follows:

- o a scalar object has only a single instance. A reference to this instance is designated by . 0, following the object identifier.
- o a tabular object has multiple instances that are related to each other. Tables in the MIB associate these instances. References to these instances typically are designated by . 1, . 2, and so forth, following the object identifier.

24.2.3 Management Information Base Systems and Interface (MIB-II)

The standard MIB-II (Management Information Base systems and interface) objects are programmed into the Canopy modules. To read this MIB, see *Management Information Base for Network Management of TCP/IP-based Internets: MIB II*, RFC 1213 at <http://www.faqs.org/rfcs/rfc1213.html>.

The MIB-II standard categorizes each object as one of the types defined in [Table 61](#).

Table 61: Categories of MIB-II objects

| Objects in category... | Control or identify the status of... |
|------------------------|---|
| system | system operations in the module. |
| interfaces | the network interfaces for which the module is configured. |
| ip | Internet Protocol information in the module. |
| icmp | Internet Control Message Protocol information in the module. (These messages flag IP problems and allow IP links to be tested.) |
| tcp | Transport Control Protocol information in the module (to control and ensure the flow of data on the Internet). |
| udp | User Datagram Protocol information in the module (for checksum and address). |

24.2.4 Canopy Enterprise MIB

The Canopy Enterprise MIB provides additional reporting and control, extending the objects for any NMS that uses SNMP interaction. This MIB comprises five text files that are formatted in standard ASN.1 (Abstract Syntax Notation One) language.

To use this MIB, perform the following steps.

Procedure 39: Installing the Canopy Enterprise MIB files

1. On the NMS, immediately beneath the `root` directory, create directory `mibviewer`.
2. Immediately beneath the `mibviewer` directory, create directory `canopymibs`.
3. Download the following three standard MIB files from the Internet Engineering Task Force at <http://www.simpleweb.org/ietf/mibs> into the `mibviewer/canopymibs` directory on the NMS:
 - SNMPv2-SMI.txt, which defines the Structure of Management Information specifications.
 - SNMPv2-CONF.txt, which allows macros to be defined for object group, notification group, module compliance, and agent capabilities.
 - SNMPv2-TC.txt, which defines general textual conventions.
4. Move the following five files from your Canopy software package directory into the `mibviewer/canopymibs` directory on the NMS (if necessary, first download the software package from <http://www.motorola.com/canopy>):
 - `whisp-tcv2-mib.txt` (Textual Conventions MIB), which defines Canopy system-specific textual conventions
 - `WHISP-GLOBAL-REG-MIB.txt` (Registrations MIB), which defines registrations for global items such as product identities and product components.
 - `WHISP-BOX-MIBV2-MIB.txt` (Box MIB), which defines module-level (AP, SM, and BH) objects.
 - `WHISP-APS-MIB.txt` (APs MIB), which defines objects that are specific to the AP or BH timing master.
 - `WHISP-SM-MIB.txt` (SM MIB), which defines objects that are specific to the SM or BH timing slave.
 - `CMM3-MIB.txt` (CMM3 MIB), which defines objects that are specific to the CMMmicro.



IMPORTANT!

Do not edit these MIB files in ASN.1. These files are intended for manipulation by only the NMS. However, you can view these files through a commercially available MIB viewer. Such viewers are listed under [MIB Viewers](#) on Page 407.

5. Download a selected MIB viewer into directory `mibviewer`.
6. As instructed by the user documentation that supports your NMS, import the eight MIB files that are listed above.

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

24.3 CONFIGURING MODULES FOR SNMP ACCESS

Canopy modules provide the following Configuration web page parameters in the SNMP tab. These govern SNMP access from the manager to the agent:

- **Community String**, which specifies the password for security between managers and the agent.
- **Accessing Subnet**, which specifies the subnet mask that allows managers to poll the agents.

Canopy modules can also be configured to send traps to specified IP addresses, which can be those of Prizm or NMS servers, for example. The parameter for this address is named **Trap Address**.

24.4 OBJECTS DEFINED IN THE CANOPY ENTERPRISE MIB

The Canopy Enterprise MIB defines separate sets of objects for

- all radio modules
- APs and BH timing masters
- SMs and BH timing slaves
- CMMmicros



NOTE:

The OFDM Series BHs do not support these objects. The MIBs that they support are listed under [Objects Defined in the Canopy OFDM BH Module MIB](#) on Page 404.

24.4.1 AP, SM, and BH Objects

The objects that the Canopy Enterprise MIB defines for all APs, SMs, and BHs are listed in [Table 62](#).

Table 62: Canopy Enterprise MIB objects for APs, SMs, and BHs

| AP, SM, BH Object Name | Value Syntax | Operation Allowed |
|--------------------------|---------------|-------------------|
| addVlanMember | Integer | manage |
| agingTimeout | Integer | manage |
| allowVIDAccess | Integer | manage |
| antennaGain ¹ | Integer | manage |
| bridgeEnable | Integer | manage |
| clearEventLog | Integer | manage |
| codePoint ² | Integer | manage |
| commString | DisplayString | manage |
| deleteUser | DisplayString | manage |

| AP, SM, BH Object Name | Value Syntax | Operation Allowed |
|-----------------------------|---------------|-------------------|
| dynamicLearning | Integer | manage |
| eirp ³ | Integer | manage |
| extFilterDelay | Integer | manage |
| fecEnable | Integer | manage |
| lanDhcpState | Integer | manage |
| managementVID | Integer | manage |
| mngtIP | IpAddress | manage |
| powerControl | Integer | manage |
| reboot | Integer | manage |
| removeVlanMember | Integer | manage |
| scheduling | Integer | manage |
| sessionTimeout | Integer | manage |
| setDefaultPlug | Integer | manage |
| subnetMask | Integer | manage |
| taggedFrame ⁴ | Integer | manage |
| transmitterOP | Integer | manage |
| trapIP ⁵ | IpAddress | manage |
| twoXRate | Integer | manage |
| userAccessLevel | Integer | manage |
| userName | DisplayString | manage |
| userPassword | DisplayString | manage |
| vlanMemberSource | Integer | manage |
| accessLevel | Integer | monitor |
| boxDeviceType | DisplayString | monitor |
| boxDeviceTypeID | DisplayString | monitor |
| boxEncryption | DisplayString | monitor |
| boxFrequency | DisplayString | monitor |
| boxTemperature ⁶ | DisplayString | monitor |
| dhcpLanIP | IpAddress | monitor |
| dhcpLanGateway | IpAddress | monitor |
| dhcpLanSubnetMask | IpAddress | monitor |
| dhcpRfPublicIP | IpAddress | monitor |
| dhcpRfPublicGateway | IpAddress | monitor |
| dhcpRfPublicSubnetMask | IpAddress | monitor |

| AP, SM, BH Object Name | Value Syntax | Operation Allowed |
|-----------------------------------|---------------------|------------------------------|
| etherLinkStatus | DisplayString | monitor |
| inSyncCount | Integer | monitor |
| lanDhcpStatus | DisplayString | monitor |
| outSyncCount | Integer | monitor |
| platformType | Integer | monitor |
| platformVer | Integer | monitor |
| pllOutLockCount | Integer | monitor |
| rfPublicDhcpStatus | DisplayString | monitor |
| txCalFailure | Integer | monitor |
| userLoginName | DisplayString | monitor |
| userPswd | DisplayString | monitor |
| whispBoxBoot | DisplayString | monitor |
| whispBoxEsn | WhispMACAddress | monitor |
| whispBoxEvntLog | EventString | monitor |
| whispBoxFPGAVer | DisplayString | monitor |
| whispBridgeAge | Integer | monitor |
| whispBridgeDesLuid | WhispLUID | monitor |
| whispBridgeExt | Integer | monitor |
| whispBridgeHash | Integer | monitor |
| whispBridgeMacAddr | MacAddress | monitor |
| whispBridgeTbErr | Integer | monitor |
| whispBridgeTbFree | Integer | monitor |
| whispBridgeTbUsed | Integer | monitor |
| whispVAge | Integer | monitor |

| AP, SM, BH Object Name | Value Syntax | Operation Allowed |
|---|---------------|-------------------|
| whispVID | Integer | monitor |
| whispVType | DisplayString | monitor |
| <p>NOTES:</p> <ol style="list-style-type: none"> For only 5.7-GHz radios. Where <i>n</i> is any number, 0 through 63. codePoint0, codePoint48, and codePoint56 can be only monitored. Deprecated. Replaced by frameType. Where <i>n</i> is any number, 1 through 10. The value of this object <i>does not</i> accurately reflect the temperature inside the module for comparison with the operating range. However, it can be helpful as one of many troubleshooting indicators. Although modules no longer report the Temperature field in the GUI, the agent in the modules continues to support this object. | | |

24.4.2 AP and BH Timing Master Objects

The objects that the Canopy Enterprise MIB defines for each AP and BH Timing Master are listed in [Table 63](#). The traps provided in this set of objects are listed under [Traps Provided in the Canopy Enterprise MIB](#) on [Page 406](#).

Table 63: Canopy Enterprise MIB objects for APs and BH timing masters

| AP, BHM Object Name | Value Syntax | Operation Allowed |
|---------------------|---------------|-------------------|
| allowedIPAccess1 | IpAddress | manage |
| allowedIPAccess2 | IpAddress | manage |
| allowedIPAccess3 | IpAddress | manage |
| apBeaconInfo | Integer | manage |
| apTwoXRate | Integer | manage |
| asIP1 | IpAddress | manage |
| asIP2 | IpAddress | manage |
| asIP3 | IpAddress | manage |
| authKey | DisplayString | manage |
| authMode | Integer | manage |
| configSource | Integer | manage |
| dAcksReservHigh | Integer | manage |
| defaultGw | IpAddress | manage |
| dfsConfig | Integer | manage |
| dwnLnkData | Integer | manage |
| dwnLnkDataRate | Integer | manage |

| AP, BHM Object Name | Value Syntax | Operation Allowed |
|--------------------------------|---------------------|------------------------------|
| dwnLnkLimit | Integer | manage |
| encryptDwBroadcast | Integer | manage |
| encryptionMode | Integer | manage |
| gpsInput | Integer | manage |
| gpsTrap | Integer | manage |
| highPriorityUpLnkPct | Integer | manage |
| ipAccessFilterEnable | Integer | manage |
| lanIp | IpAddress | manage |
| lanMask | IpAddress | manage |
| limitFreqBand900 | Integer | manage |
| linkTestAction ¹ | Integer | manage |
| linkTestDuration | Integer | manage |
| linkTestLUID | Integer | manage |
| maxRange | Integer | manage |
| ntpServerIP | IpAddress | manage |
| numCtlSlots | Integer | manage |
| numCtlSlotsHW | Integer | manage |
| numCtlSlotsReserveHigh | Integer | manage |
| numDAckSlots | Integer | manage |
| numUAckSlots | Integer | manage |
| privateIp | IpAddress | manage |
| regTrap | Integer | manage |
| rfFreqCarrier | Integer | manage |
| sectorID | Integer | manage |
| sesHiDownCIR | Integer | manage |
| sesHiUpCIR | Integer | manage |
| sesLoDownCIR | Integer | manage |
| sesHiDownCIR | Integer | manage |
| smlIsolation | Integer | manage |
| tslBridging | Integer | manage |
| txSpreading | Integer | manage |
| uAcksReservHigh | Integer | manage |
| untranslatedArp | Integer | manage |
| updateAppAddress | IpAddress | manage |

| AP, BHM Object Name | Value Syntax | Operation Allowed |
|--------------------------------|---------------------|------------------------------|
| upLnkDataRate | Integer | manage |
| upLnkLimit | Integer | manage |
| vlanEnable | Integer | manage |
| actDwnFragCount | Gauge32 | monitor |
| actDwnLinkIndex | Integer | monitor |
| actUpFragCount | Gauge32 | monitor |
| adaptRate | DisplayString | monitor |
| avgPowerLevel | DisplayString | monitor |
| dataSlotDwn | Integer | monitor |
| dataSlotUp | Integer | monitor |
| dataSlotUpHi | Integer | monitor |
| dfsStatus | DisplayString | monitor |
| downLinkEff | Integer | monitor |
| downLinkRate | Integer | monitor |
| dwnLnkAckSlot | Integer | monitor |
| dwnLnkAckSlotHi | Integer | monitor |
| expDwnFragCount | Gauge32 | monitor |
| expUpFragCount | Gauge32 | monitor |
| fpgaVersion | DisplayString | monitor |
| gpsStatus | DisplayString | monitor |
| lastPowerLevel | DisplayString | monitor |
| linkAirDelay | Integer | monitor |
| linkAveJitter | Integer | monitor |
| linkDescr | DisplayString | monitor |
| linkESN | PhysAddress | monitor |
| linkInDiscards | Counter32 | monitor |
| linkInError | Counter32 | monitor |
| linkInNUcastPkts | Counter32 | monitor |
| linkInOctets | Counter32 | monitor |
| linkInUcastPkts | Counter32 | monitor |
| linkInUnknownProtos | Counter32 | monitor |
| linkLastJitter | Integer | monitor |
| linkLastRSSI | Integer | monitor |
| linkLUID | Integer | monitor |

| AP, BHM Object Name | Value Syntax | Operation Allowed |
|--------------------------------|---------------------|------------------------------|
| linkMtu | Integer | monitor |
| linkOutDiscards | Counter32 | monitor |
| linkOutError | Counter32 | monitor |
| linkOutNUcastPkts | Counter32 | monitor |
| linkOutOctets | Counter32 | monitor |
| linkOutQLen | Gauge32 | monitor |
| linkOutUcastPkts | Counter32 | monitor |
| linkRegCount | Integer | monitor |
| linkReRegCount | Integer | monitor |
| linkRSSI | Integer | monitor |
| linkSessState | Integer | monitor |
| linkSiteName | DisplayString | monitor |
| linkSpeed | Gauge32 | monitor |
| linkTestError | DisplayString | monitor |
| linkTestStatus | DisplayString | monitor |
| linkTimeOut | Integer | monitor |
| maxDwnLinkIndex | Integer | monitor |
| numCtrSlot | Integer | monitor |
| numCtrSlotHi | Integer | monitor |
| PhysAddress | PhysAddress | monitor |
| radioSlicing | Integer | monitor |
| radioTxGain | Integer | monitor |
| regCount | Integer | monitor |
| sesDownlinkLimit | Integer | monitor |
| sesDownlinkRate | Integer | monitor |
| sesUplinkLimit | Integer | monitor |
| sesUplinkRate | Integer | monitor |
| sessionCount | Integer | monitor |
| softwareBootVersion | DisplayString | monitor |
| softwareVersion | DisplayString | monitor |
| testDuration | Integer | monitor |
| testLUID | Integer | monitor |
| upLinkEff | Integer | monitor |
| upLinkRate | Integer | monitor |

| AP, BHM Object Name | Value Syntax | Operation Allowed |
|---|--------------|-------------------|
| upLnkAckSlot | Integer | monitor |
| upLnkAckSlotHi | Integer | monitor |
| whispGPSStats | Integer | monitor |
| NOTES: | | |
| 1. You can set to 1 to initiate a link test, but not 0 to stop. The value 0 is only an indication of the idle link test state. | | |

24.4.3 SM and BH Timing Slave Objects

The objects that the Canopy Enterprise MIB defines for each SM and BH Timing Slave are listed in [Table 64](#).

Table 64: Canopy Enterprise MIB objects for SMs and BH timing slaves

| SM, BHS Object Name | Value Syntax | Operation Allowed |
|---------------------|---------------|-------------------|
| allOtherIPFilter | Integer | manage |
| allOthersFilter | Integer | manage |
| allowedIPAccess1 | IpAddress | manage |
| allowedIPAccess2 | IpAddress | manage |
| allowedIPAccess3 | IpAddress | manage |
| alternateDNSIP | IpAddress | manage |
| arpCacheTimeout | Integer | manage |
| arpFilter | Integer | manage |
| authKey | DisplayString | manage |
| authKeyOption | Integer | manage |
| bootpcFilter | Integer | manage |
| bootpsFilter | Integer | manage |
| defaultGw | IpAddress | manage |
| dhcpClientEnable | Integer | manage |
| dhcpIPStart | IpAddress | manage |
| dhcpNumIPsToLease | Integer | manage |
| dhcpServerEnable | Integer | manage |
| dhcpServerLeaseTime | Integer | manage |
| dmzEnable | Integer | manage |
| dmzIP | IpAddress | manage |
| dnsAutomatic | Integer | manage |
| enable8023link | Integer | manage |

| SM, BHS Object Name | Value Syntax | Operation Allowed |
|--------------------------------|---------------------|------------------------------|
| ethAccessFilterEnable | Integer | manage |
| hiPriorityChannel | Integer | manage |
| hiPriorityDownlinkCIR | Integer | manage |
| hiPriorityUplinkCIR | Integer | manage |
| ingressVID | Integer | manage |
| ip4MultFilter | Integer | manage |
| ipAccessFilterEnable | Integer | manage |
| lanIp | IpAddress | manage |
| lanMask | IpAddress | manage |
| localIP | IpAddress | manage |
| lowPriorityDownlinkCIR | Integer | manage |
| lowPriorityUplinkCIR | Integer | manage |
| naptEnable | Integer | manage |
| naptPrivateIP | IpAddress | manage |
| naptPrivateSubnetMask | IpAddress | manage |
| naptPublicGatewayIP | IpAddress | manage |
| naptPublicIP | IpAddress | manage |
| naptPublicSubnetMask | IpAddress | manage |
| naptRFPublicGateway | IpAddress | manage |
| naptRFPublicIP | IpAddress | manage |
| naptRFPublicSubnetMask | IpAddress | manage |
| networkAccess | Integer | manage |
| port | Integer | manage |
| port1TCPFilter | Integer | manage |
| port2TCPFilter | Integer | manage |
| port3TCPFilter | Integer | manage |
| port1UDPFilter | Integer | manage |
| port2UDPFilter | Integer | manage |
| port3UDPFilter | Integer | manage |
| powerUpMode | Integer | manage |
| pppoeFilter | Integer | manage |
| preferredDNSIP | IpAddress | manage |
| protocol | Integer | manage |
| radioDbmInt | Integer | manage |

| SM, BHS Object Name | Value Syntax | Operation Allowed |
|--------------------------------|---------------------|------------------------------|
| rfDhcpState | Integer | manage |
| rfScanList | DisplayString | manage |
| smbFilter | Integer | manage |
| snmpFilter | Integer | manage |
| tcpGarbageCollectTmout | Integer | manage |
| timingPulseGated | Integer | manage |
| twoXRate | Integer | manage |
| udpGarbageCollectTmout | Integer | manage |
| uplinkBCastFilter | Integer | manage |
| userDefinedPort1 | Integer | manage |
| userDefinedPort2 | Integer | manage |
| userDefinedPort3 | Integer | manage |
| userP1Filter | Integer | manage |
| userP2Filter | Integer | manage |
| userP3Filter | Integer | manage |
| adaptRate | DisplayString | monitor |
| airDelay | Integer | monitor |
| calibrationStatus | DisplayString | monitor |
| dhcpcdns1 | IpAddress | monitor |
| dhcpcdns2 | IpAddress | monitor |
| dhcpcdns3 | IpAddress | monitor |
| dhcpCip | IpAddress | monitor |
| dhcpClientLease | TimeTicks | monitor |
| dhcpCSMask | IpAddress | monitor |
| dhcpDfltRterIP | IpAddress | monitor |
| dhcpDomName | DisplayString | monitor |
| dhcpServerTable | DhcpServerEntry | monitor |
| dhcpSip | IpAddress | monitor |
| hostIp | IpAddress | monitor |
| hostLease | TimeTicks | monitor |
| hostMacAddress | PhysAddress | monitor |
| jitter | Integer | monitor |
| radioDbm | DisplayString | monitor |
| radioSlicing | Integer | monitor |

| SM, BHS Object Name | Value Syntax | Operation Allowed |
|---------------------|---------------|-------------------|
| radioTxGain | Integer | monitor |
| registeredToAp | DisplayString | monitor |
| rsi | Integer | monitor |
| sessionStatus | DisplayString | monitor |

24.4.4 CMMmicro Objects

The objects that the Canopy Enterprise MIB defines for each CMMmicro are listed in [Table 65](#).

Table 65: Canopy Enterprise MIB objects for CMMmicros

| CMMmicro Object Name | Value Syntax | Operation Allowed |
|----------------------|---------------|-------------------|
| clearEventLog | Integer | manage |
| defaultGateWay | IpAddress | manage |
| displayOnlyAccess | DisplayString | manage |
| fullAccess | DisplayString | manage |
| gpsTimingPulse | Integer | manage |
| lan1Ip | IpAddress | manage |
| lan1SubnetMask | IpAddress | manage |
| port1Config | Integer | manage |
| port1Description | DisplayString | manage |
| port1PowerCtr | Integer | manage |
| port2Config | Integer | manage |
| port2Description | DisplayString | manage |
| port2PowerCtr | Integer | manage |
| port3Config | Integer | manage |
| port3Description | DisplayString | manage |
| port3PowerCtr | Integer | manage |
| port4Config | Integer | manage |
| port4Description | DisplayString | manage |
| port4PowerCtr | Integer | manage |
| port5Config | Integer | manage |
| port5Description | DisplayString | manage |
| port5PowerCtr | Integer | manage |
| port6Config | Integer | manage |
| port6Description | DisplayString | manage |

| CMMmicro Object Name | Value Syntax | Operation Allowed |
|-----------------------------|---------------------|--------------------------|
| port6PowerCtr | Integer | manage |
| port7Config | Integer | manage |
| port7Description | DisplayString | manage |
| port7PowerCtr | Integer | manage |
| port8Config | Integer | manage |
| port8Description | DisplayString | manage |
| port8PowerCtr | Integer | manage |
| reboot | Integer | manage |
| webAutoUpdate | Integer | manage |
| deviceType | DisplayString | monitor |
| displayOnlyStatus | DisplayString | monitor |
| duplexStatus | Integer | monitor |
| eventLog | EventString | monitor |
| fullAccessStatus | DisplayString | monitor |
| gpsAntennaConnection | DisplayString | monitor |
| gpsDate | DisplayString | monitor |
| gpsHeight | DisplayString | monitor |
| gpsInvalidMsg | DisplayString | monitor |
| gpsLatitude | DisplayString | monitor |
| gpsLongitude | DisplayString | monitor |
| gpsReceiverInfo | DisplayString | monitor |
| gpsRestartCount | Integer | monitor |
| gpsSatellitesTracked | DisplayString | monitor |
| gpsSatellitesVisible | DisplayString | monitor |
| gpsTime | DisplayString | monitor |
| gpsTrackingMode | DisplayString | monitor |
| height | DisplayString | monitor |
| latitude | DisplayString | monitor |
| linkSpeed | Integer | monitor |
| linkStatus | Integer | monitor |
| longitude | DisplayString | monitor |
| macAddress | DisplayString | monitor |
| pkts1024to1522Octets | Counter32 | monitor |
| pkts128to255Octets | Counter32 | monitor |

| CMMmicro Object Name | Value Syntax | Operation Allowed |
|---------------------------------|---------------------|------------------------------|
| pkts256to511Octets | Counter32 | monitor |
| pkts512to1023Octets | Counter32 | monitor |
| pkts64Octets | Counter32 | monitor |
| pkts65to127Octets | Counter32 | monitor |
| pldVersion | DisplayString | monitor |
| portIndex | Integer | monitor |
| portNumber | Integer | monitor |
| powerStatus | Integer | monitor |
| rxAlignmentErrors | Counter32 | monitor |
| rxBroadcastPkts | Counter32 | monitor |
| rxDropPkts | Counter32 | monitor |
| rxExcessSizeDisc | Counter32 | monitor |
| rxFCSErrors | Counter32 | monitor |
| rxFragments | Counter32 | monitor |
| rxGoodOctets | Counter64 | monitor |
| rxJabbers | Counter32 | monitor |
| rxMulticastPkts | Counter32 | monitor |
| rxOctets | Counter64 | monitor |
| rxOversizePkts | Counter32 | monitor |
| rxPausePkts | Counter32 | monitor |
| rxSAChanges | Counter32 | monitor |
| rxSymbolErrors | Counter32 | monitor |
| rxUndersizePkts | Counter32 | monitor |
| rxUnicastPkts | Counter32 | monitor |
| satellitesTracked | DisplayString | monitor |
| satellitesVisible | DisplayString | monitor |
| softwareVersion | DisplayString | monitor |
| syncStatus | DisplayString | monitor |
| systemTime | DisplayString | monitor |
| trackingMode | DisplayString | monitor |
| txBroadcastPkts | Counter32 | monitor |
| txCollisions | Counter32 | monitor |
| txDeferredTransmit | Counter32 | monitor |
| txDropPkts | Counter32 | monitor |

| CMMmicro Object Name | Value Syntax | Operation Allowed |
|-----------------------------|---------------------|--------------------------|
| txExcessiveCollision | Counter32 | monitor |
| txFrameInDisc | Counter32 | monitor |
| txLateCollision | Counter32 | monitor |
| txMulticastPkts | Counter32 | monitor |
| txMultipleCollision | Counter32 | monitor |
| txOctets | Counter64 | monitor |
| txPausePkts | Counter32 | monitor |
| txSingleCollision | Counter32 | monitor |
| txUnicastPkts | Counter32 | monitor |
| upTime | DisplayString | monitor |

24.5 OBJECTS DEFINED IN THE CANOPY OFDM BH MODULE MIB

The objects that the Canopy OFDM BH module MIB defines are listed in [Table 67](#).

Table 66: Canopy OFDM BH module MIB objects

| Object Name | Value Syntax | Operation Allowed |
|-------------------------------|---------------------|--------------------------|
| ipAddress | IpAddress | manage |
| subnetMask | IpAddress | manage |
| gatewayIpAddress | IpAddress | manage |
| targetMACAddress ¹ | DisplayString | manage |
| masterSlaveMode | Integer | manage |
| maximumTransmitPower | Integer | manage |
| receivePower ² | Integer | manage |
| vectorError ² | Integer | manage |
| transmitPower ² | Integer | manage |
| range | Integer | manage |
| linkLoss ² | Integer | manage |
| receiveChannel | Integer | manage |
| transmitChannel | Integer | manage |
| receiveModulationMode | Integer | manage |
| transmitModulationMode | Integer | manage |
| receiveSnr ² | Integer | manage |
| systemReset | Integer | monitor |

| Object Name | Value Syntax | Operation Allowed |
|--|---------------|-------------------|
| softwareVersion | DisplayString | monitor |
| hardwareVersion | DisplayString | monitor |
| NOTES: | | |
| 1. Of the other BH in the link. | | |
| 2. <i>max, mean, min, last</i> during the past hour. | | |

24.6 OBJECTS SUPPORTED IN THE CANOPY 30/60-Mbps BH

The 30/60-Mbps BH supports the following MIBs:

- MIB II, RFC 1213, System Group
- MIB II, RFC 1213, Interfaces Group
- WiMAX 802.16 WMAN-IF-MIB
- Bridge MIB, RFC 1493, dot1dBaseGroup
- Bridge MIB, RFC 1493, dot1dBasePortTableGroup
- 30/60-Mbps Backhaul Canopy proprietary MIB

24.7 OBJECTS SUPPORTED IN THE CANOPY 150/300-Mbps BH

The 150/300-Mbps BH supports the following MIBs:

- MIB II, RFC 1213, System Group
- MIB II, RFC 1213, Interfaces Group
- WiMAX 802.16 WMAN-IF-MIB
- Bridge MIB, RFC 1493, dot1dBaseGroup
- Bridge MIB, RFC 1493, dot1dBasePortTableGroup
- High-capacity counter MIB, RFC 2233
- 150/300-Mbps Backhaul Canopy proprietary MIB

24.8 INTERFACE DESIGNATIONS IN SNMP

SNMP identifies the ports of the module as follows:

- Interface 1 represents the Ethernet interface of the module. To monitor the status of Interface 1 is to monitor the traffic on the Ethernet interface.
- Interface 2 represents the RF interface of the module. To monitor the status of Interface 2 is to monitor the traffic on the RF interface.

These interfaces can be viewed on the NMS through definitions that are provided in the standard MIB files.

24.9 TRAPS PROVIDED IN THE CANOPY ENTERPRISE MIB

Canopy modules provide the following SNMP traps for automatic notifications to the NMS:

- `whispGPSInSync`, which signals a transition from not synchronized to synchronized.
- `whispGPSOutSync`, which signals a transition from synchronized to not synchronized.
- `whispRegComplete`, which signals registration completed.
- `whispRegLost`, which signals registration lost.
- `whispRadarDetected`, which signals that the one-minute scan has been completed, radar has been detected, and the radio will shutdown.
- `whispRadarEnd`, which signals that the one-minute scan has been completed, radar *has not* been detected, and the radio will resume normal operation.



NOTE:

The OFDM Series BHs do not support the traps listed above.

24.10 TRAPS PROVIDED IN THE CANOPY 30/60-Mbps BH MODULE MIB

Canopy 30/60-Mbps BH modules provide the following SNMP traps for automatic notifications to the NMS:

- `coldStart`
- `linkUp`
- `linkDown`
- `dfsChannelChange`, which signals that the channel has changed.
- `dfsImpulsiveInterferenceDetected`, which signals that impulsive interference has been detected.

24.11 TRAPS PROVIDED IN THE CANOPY 150/300-Mbps BH MODULE MIB

Canopy 150/300-Mbps BH modules provide the following SNMP traps for automatic notifications to the NMS:

- `coldStart`
- `linkUp`
- `linkDown`
- `dfsChannelChange`, which signals that the channel has changed.
- `dfsImpulsiveInterferenceDetected`, which signals that impulsive interference has been detected.

24.12 MIB VIEWERS

Any of several commercially available MIB viewers can facilitate management of these objects through SNMP. Some are available as open source software. The Canopy division does not endorse, support, or discourage the use of any these viewers.

To assist end users in this area, Canopy offers a starter guide for one of these viewers—MRTG (Multi Router Traffic Grapher). This starter guide is titled *Canopy Network Management with MRTG: Application Note*, and is available in the Document Library section under Support at <http://www.motorola.com/canopy>. MRTG software is available at <http://mrtg.hdl.com/mrtg.html>.

Other MIB viewers are available and/or described at the following web sites:

<http://ns3.ndgsoftware.com/Products/NetBoy30/mibbrowser.html>

<http://www.adventnet.com/products/snmputilities/>

<http://www.dart.com/samples/mib.asp>

<http://www.edge-technologies.com/webFiles/products/nvision/index.cfm>

<http://www.ipswitch.com/products/whatsup/monitoring.html>

<http://www.koshna.com/products/KMB/index.asp>

<http://www.mg-soft.si/mgMibBrowserPE.html>

<http://www.mibexplorer.com>

<http://www.netmechanica.com/mibbrowser.html>

<http://www.networkview.com>

<http://www.newfreeware.com/search.php3?q=MIB+browser>

<http://www.nudesignteam.com/walker.html>

<http://www.oidview.com/oidview.html>

<http://www.solarwinds.net/Tools>

<http://www.stargus.com/solutions/xray.html>

<http://www.totilities.com/Products/MibSurfer/MibSurfer.htm>

25 USING THE CANOPY NETWORK UPDATER TOOL (CNUT)

The Canopy Network Updater Tool manages and automates the software and firmware upgrade process for Canopy radio and CMMmicro modules across the network. This eliminates the need for an administrator to visit each radio in the network (or each AP while using the Autoupdate feature) to upgrade the modules.

25.1 CNUT FUNCTIONS

The Canopy Network Updater Tool

- automatically discovers all Canopy network elements
- executes a UDP command that initiates and terminates the Autoupdate mode within APs. This command is both secure and convenient:
 - For security, the AP accepts this command from only the IP address that you specify in the Configuration page of the AP.
 - For convenience, Network Updater automatically sets this Configuration parameter in the APs to the IP address of the Network Updater server when the server performs any of the update commands.
- allows you to choose among updating
 - your entire network.
 - only elements that you select.
 - only network branches that you select.
- provides a Script Engine that you can use with any script that
 - you define.
 - Canopy supplies.

25.2 NETWORK ELEMENT GROUPS

With the Canopy Network Updater Tool, you can identify element groups composed of network elements that you select. Identifying these element groups

- organizes the display of elements (for example, by region or by AP cluster).
- allows you to
 - perform an operation on all elements in the group simultaneously.
 - set group-level defaults for telnet or ftp password access and SNMP Community String (defaults that can be overridden in an individual element when necessary).

25.3 NETWORK LAYERS

A typical Canopy network contains multiple layers of elements, each layer lying farther from the Point of Presence. For example, SMs are behind an AP and thus, in this context, at a lower layer than the AP. Correctly portraying these layers in Network Updater is essential so that Network Updater can perform radio and AP cluster upgrades in an appropriate order.

**IMPORTANT!**

Correct layer information ensures that Network Updater does not command an AP that is behind another AP/SM pair (such as in a remote AP installation) to perform an upgrade at the same time as the SM that is feeding the AP. If this occurs, then the remote AP loses network connection during the upgrade (when the SM in front of the AP completes its upgrade and reboots).

25.4 SCRIPT ENGINE

Script Engine is the capability in Network Updater that executes any user-defined script against any network element or element group. This capability is useful for network management, especially for scripts that you repetitively execute across your network.

The Autodiscovery capability in Network Updater finds all of your Canopy network elements. This comprehensive discovery

- ensures that, when you intend to execute a script against *all* elements, the script is indeed executed against *all* elements.
- maintains master lists of elements (element groups) against which you selectively execute scripts.

The following scripts are included with CNUT:

- AP Data Import from BAM
- AP Data Export to BAM
- Set Autoupdate Address on APs
- Set SNMP Accessibility
- Reset Unit

25.5 SOFTWARE DEPENDENCIES FOR CNUT

CNUT functionality requires

- one of the following operating systems
 - Windows® 2000
 - Windows XP
 - Red Hat Linux 9
 - Red Hat Enterprise Linux Version 3
- Java™ Runtime Version 1.4.2 or later
- Perl 5.8.0 or ActivePerl 5.8.3 software or later

25.6 CNUT DOWNLOAD

CNUT can be downloaded together with each Canopy system release that supports CNUT. Software for these Canopy system releases is packaged on the Canopy Support web page as either

- a `.zip` file for use without the CNUT application.
- a `.pkg` file that the CNUT application can open.

26 USING INFORMATIONAL TABS IN THE GUI

26.1 VIEWING GENERAL STATUS (ALL)

See

- [General Status Tab of the AP](#) on Page 201.
- [General Status Tab of the SM](#) on Page 198.
- [General Status Tab of the BHM](#) on Page 213.
- [Beginning the Test of Point-to-Point Links](#) on Page 210.

26.2 VIEWING SESSION STATUS (AP, BHM)

The Session Status tab in the Home page provides information about each SM that has registered to the AP. This information is useful for managing and troubleshooting a Canopy system. This tab also includes the current active values on each SM for MIR, CIR, and VLAN, as well as the source of these values, representing the SM itself, BAM, or the AP and cap.

An example of the Session Status tab is displayed in [Figure 148](#).

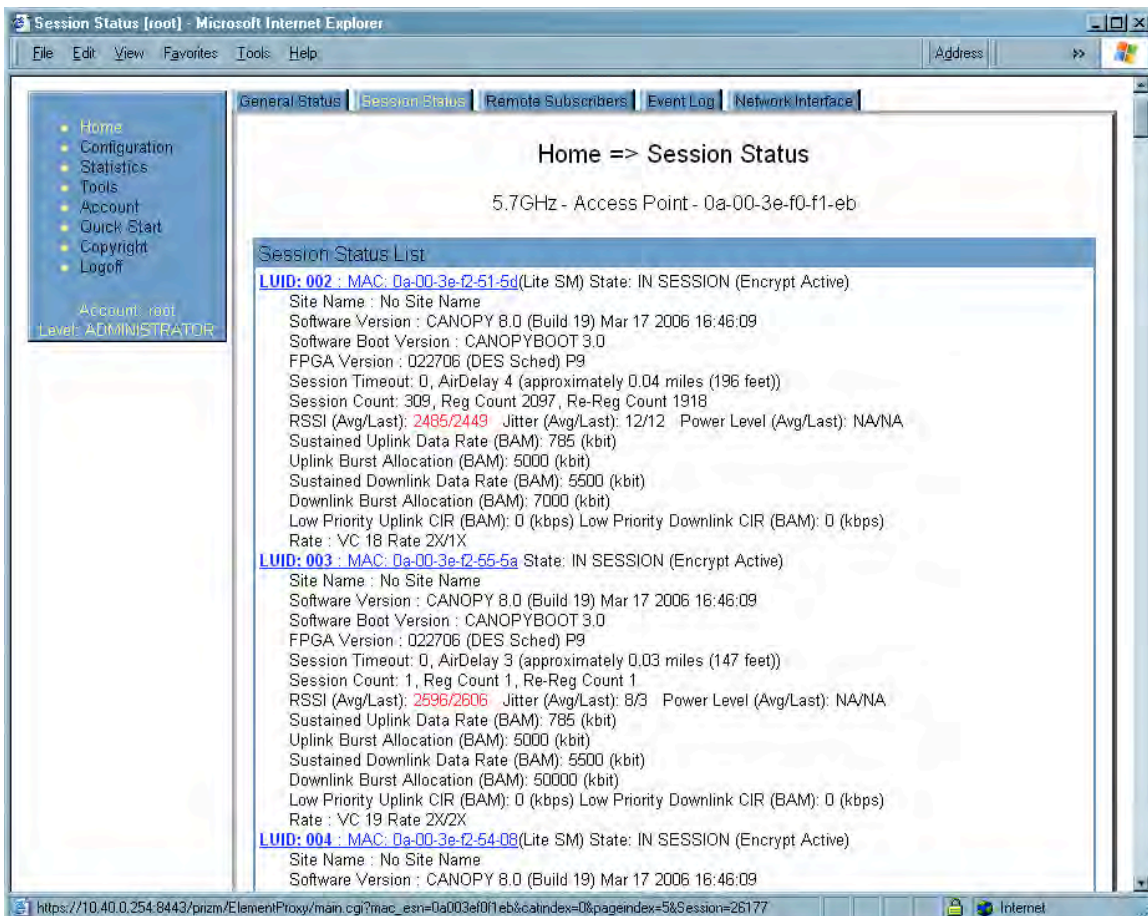


Figure 148: Session Status tab data, example

An additional example and explanations of the fields on this tab are provided in [Session Status Tab of the AP](#) on Page 193.

26.3 VIEWING REMOTE SUBSCRIBERS (AP, BHM)

See

- [Remote Subscribers Tab of the AP](#) on Page 197.
- [Continuing the Test of Point-to-Point Links](#) on Page 212.

26.4 INTERPRETING MESSAGES IN THE EVENT LOG (ALL)

Each line in the Event Log of a module Home page begins with a time and date stamp. However, some of these lines wrap as a combined result of window width, browser preferences, and line length. You may find this tab easiest to use if you widen the window until all lines are shown as beginning with the time and date stamp.

26.4.1 Time and Date Stamp

The time and date stamp reflect either

- GPS time and date directly or indirectly received from the CMM.
- the running time and date that you have set in the Time & Date web page.

NOTE:



In the Time & Date web page, if you have left any time field or date field unset and clicked the **Set Time and Date** button, then the time and date default to 00:00:00 UT : 01/01/00.

A reboot causes the preset time to pause or, in some cases, to run in reverse. Additionally, a power cycle resets the running time and date to the default 00:00:00 UT : 01/01/00. Thus, whenever either a reboot or a power cycle has occurred, you should reset the time and date in the Time & Date web page of any module that is not set to receive sync.

26.4.2 Event Log Data Collection

The collection of event data continues through reboots and power cycles. When the buffer allowance for event log data is reached, the system adds new data into the log and discards an identical amount of the oldest data.

Each line that contains the expression WatchDog flags an event that was both

- considered by the system software to have been an exception
- recorded in the *preceding* line.

Conversely, a Fatal Error() message flags an event that is recorded in the *next* line. Some exceptions and fatal errors may be significant and require either operator action or technical support.

An example portion of Event Log data is displayed in [Figure 149](#). In this figure (unlike in the Event Log web page)

- lines are alternately highlighted to show the varying length of wrapped lines.
- the types of event messages (which follow the time and date stamps and the file and line references) are underscored as quoted in [Table 67](#) and [Table 68](#).