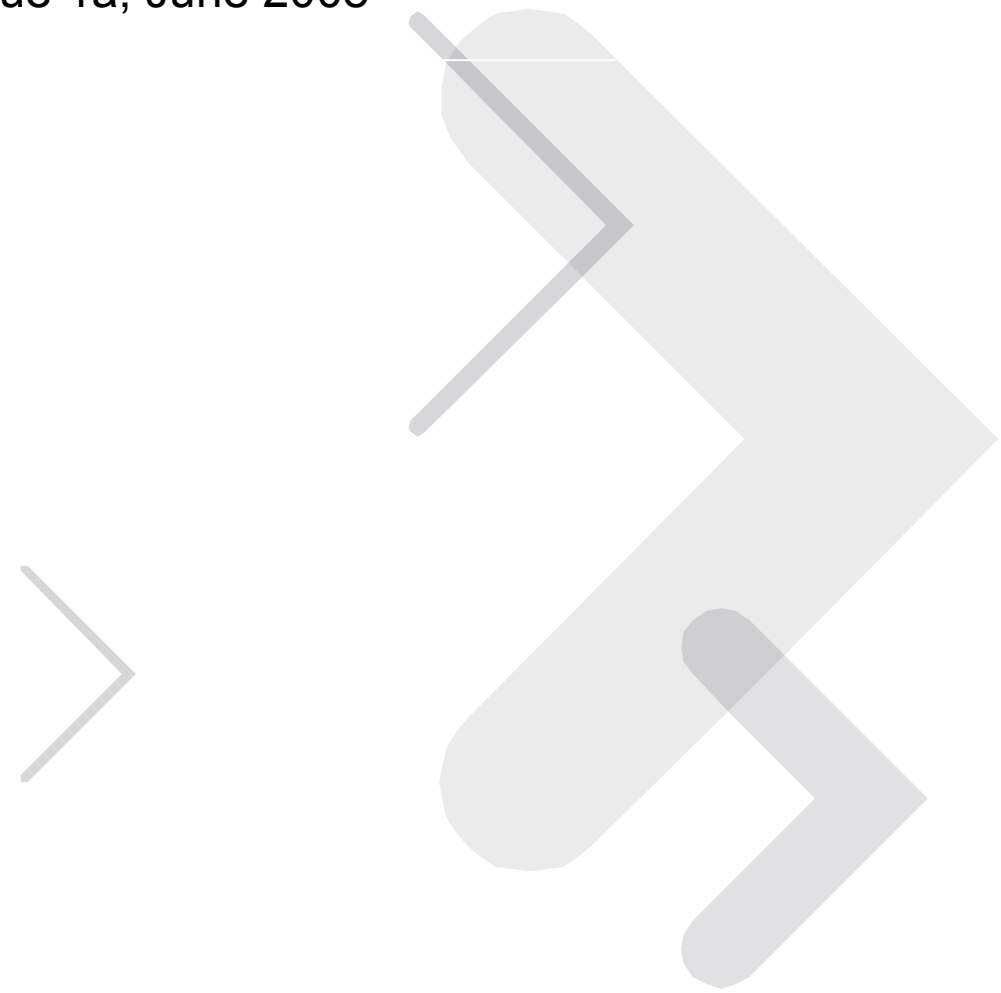
Canopy® Cluster Management Module 4 (CMM4) User Guide

Issue 1a, June 2008



Notices

See important regulatory and legal notices in Section 7 on Page 58.

Trademarks, Product Names, and Service Names

MOTOROLA, the stylized M Logo and all other trademarks indicated as such herein are trademarks of Motorola, Inc.® Reg. U.S. Pat & Tm. Office. Canopy is a registered trademark and MOTOwi4 is a trademark of Motorola, Inc. All other product or service names are the property of their respective owners.

http://www.motorola.com/canopy

TABLE OF CONTENTS

List of Tables

List of Figures

List of Procedures

1 USING THIS GUIDE

The audience for this document includes Canopy planners, engineers, installers, and technicians who need to plan for, configure, install, and operate the CMM4.

1.1 NEW IN THIS ISSUE

This section is a placeholder where future issues will announce items that are added, clarified, or corrected.

1.2 FINDING THE INFORMATION YOU NEED

1.2.1 Becoming Familiar with This Guide

The Table of Contents provides not only a sequential index of topics but also a visual glance at the organization of topics in this guide. A few minutes spent with the Table of Contents in either the paper or the electronic version of this guide can save much more time in finding information now and in the future.

Important Regulatory Information is found in Section 7.

Important Safety Information is found throughout the guide and is highlighted with appropriate icons.

1.2.2 Searching This Guide

To search this document,

- Look visually in the Table of Contents for the topic.
- Use the search capability of your PDF reader (Adobe Reader® for example) to search for desired topics. If you begin your search at the beginning of the document, your first hits are likely to be high value results from the Table of Contents.

1.3 FEEDBACK ON DOCUMENTATION

Is this document accurate, complete, and clear? How can it be improved? Please send your feedback on Canopy documentation to technical-documentation@canopywireless.com.

2 TECHNICAL SUPPORT

IMPORTANT!
Don't clear the Event Log after you encounter issues – it may be useful to Technical Support if you need to escalate the issue.

Here is the escalation path for resolution of a problem:

1. Check documentation:
   i. This document.
   ii. Release Notes for recent software releases.
   iii. Canopy System Release 8 User's Guide, available at http://motorola.canopywireless.com/support/library/
2. Consider checking the Canopy Community Forum at http://motorola.canopywireless.com/support/community.
3. Consider checking the Canopy Knowledge Base at http://motorola.canopywireless.com/support/knowledge/
4. Escalate the problem to your Canopy supplier or reseller.
5. Escalate the problem to Canopy Technical Support or other designated Tier 3 technical support:

Worldwide Canopy Technical Support

email: technical-support@canopywireless.com

1-888-605-2552 or **+1 217 824 9742**

European Canopy Technical Support

email: essc@motorola.com

+44 (0)1793 564680

Calls are logged 24 x 7, cases are worked Mon-Fri 09:00 - 17:00 GMT

When you send e-mail or call, please include, as appropriate, software release on each module, IP addresses, MAC addresses, and features enabled, like VLAN. You may be asked to run the Support Tool on CNUT or Prizm to provide a complete network picture.

3 PRODUCT DESCRIPTION

3.1 DESCRIPTION

The Cluster Management Module 4 (CMM4) (Model number 1090CK) provides power, sync, and network connectivity for up to eight APs, backhauls, and Ethernet terrestrial feeds in a variety of configurations. The CMM4 provides

- Sync over Power over Ethernet and integrated surge suppression for up to 8 Canopy Ethernet connections. The Canopy power scheme is different than the later IEEE Standard 802.3af, and is not compatible with it.
- Managed switching using a hardened EtherWAN switch with 9 ports - eight 10/100Base-T ports and one copper 10/100/1000Base-T ("Gigabit Ethernet") port. One of the 9 ports is used for providing network access to manage the CMM4 cluster controller, leaving 8 for network use.
- Surge suppression on the incoming 30-Volt DC power line and GPS coax cable.
- Auto-negotiation on the Ethernet ports. Ports will auto-negotiate to match inputs that are either 100Base-TX or 10Base-T, and either full duplex or half duplex, where the connected device is set to auto-negotiate. Alternatively, these parameters are settable.
- An always-on NTP (Network Time Protocol) server that can provide date and time to any radio or other device that can reach the CMM's management IP address.

Inside the CMM4 enclosure is a **cluster controller**, an **EtherWAN switch**, and a GPS coax surge suppressor. Figure 1 shows an external view and Figure 2 shows a detailed view of the CMM4.

The **cluster controller** injects power and synchronization on up to eight Ethernet ports and provides the equivalent of 600SSC surge suppression on each of the eight ports. The cluster controller is managed using a web browser, Telnet, or SNMP, and is supported by the Prizm Element Management System (EMS). The cluster controller receives 29/30 VDC power from the external power supply, and provides 20 VDC power for the EtherWAN switch and other auxiliary equipment. The cluster controller includes a GPS module, which provides sync and GPS information to the CMM, a management port, an override toggle switch, and an auxiliary sync port for connecting to another CMM.

The hardened, managed **EtherWAN switch** provides a full array of networking features. The EtherWAN switch can be managed using a web browser, Telnet, SNMP, or a serial interface, and is discoverable and manageable by Prizm. For information on features and configuration of the EtherWAN, see the *EtherWAN Switch Manual* available for download at http://www.EtherWAN.com/manuals/es/EX96000_e1_Manual.pdf

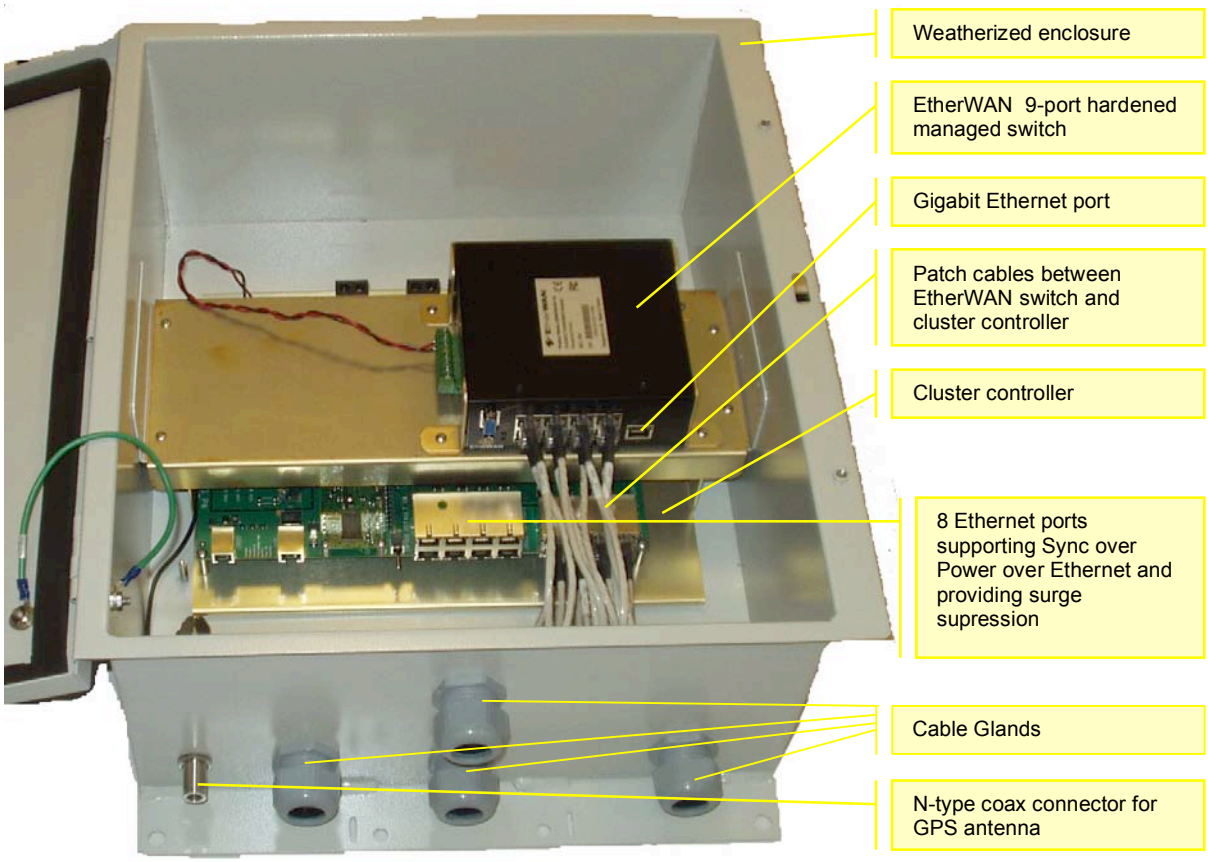


Figure 1: CMM4 External View

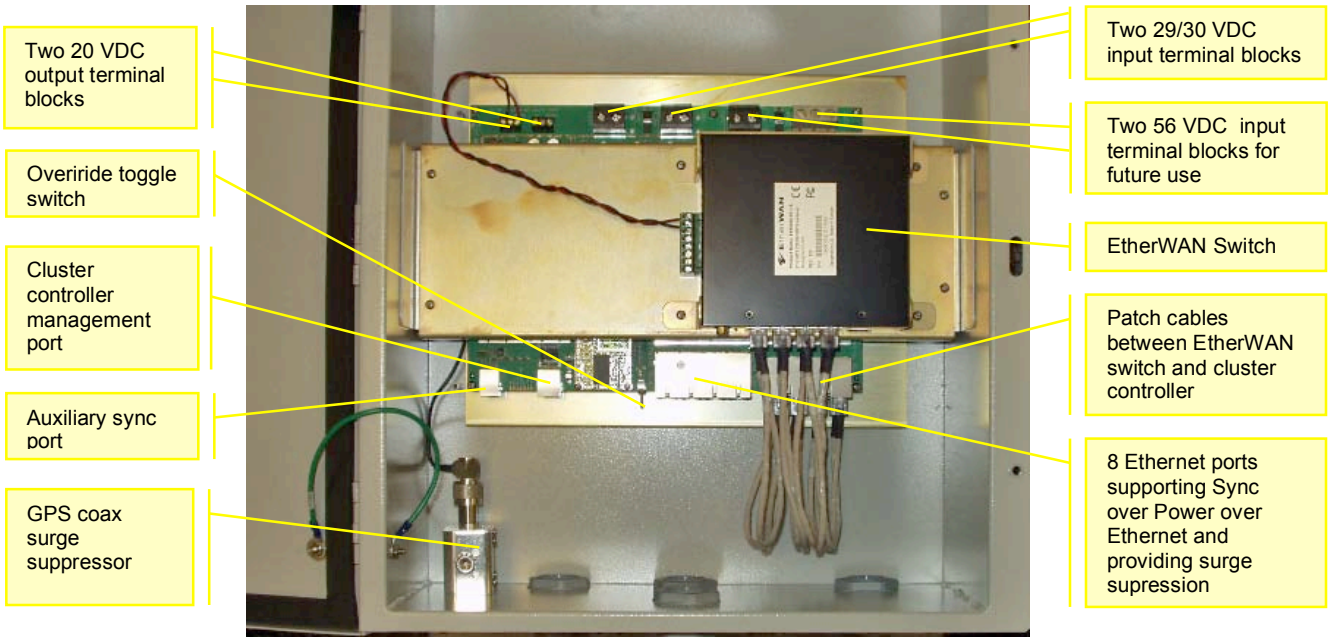


Figure 2: CMM4 Detailed View

Outside the enclosure the CMM4 requires a **GPS antenna** and a **power supply**.

The **GPS antenna** (Figure 3) requires a good view of the sky, but does not necessarily need to be mounted high on the tower. It is included with the CMM4 and is also available as a replacement item using part number GPSANTPNM03D.

Figure 3: GPS Antenna

A **30-Volt power supply** is required, and ordered separately from the CMM4. See section 3.2 for more information on the power supply.

The CMM4 (1090CK) as shipped includes:

- Weatherized enclosure containing the Cluster Controller, EtherWAN Ethernet Switch, and GPS coax surge suppressor
- Patch cables between the Cluster Controller and the EtherWAN Ethernet Switch
- U-bolts and V-brackets for pole-mounting the CMM4
- GPS Antenna
- GPS antenna pole-mount kit
- A 1-hole cable gland insert for use on the DC power cable (usually shipped attached to one of the patch cables, for convenience)
- Serial cable for connecting a PC or any device equipped with a serial port to the serial port of the EtherWAN switch

The CMM4 (1090CK) as shipped **does not** include

- The 30 V power supply needed to power the CMM4, which must be ordered separately (see section 3.2 and Table 1)
- Ethernet cables to connect the CMM4 to APs, backhauls, or terrestrial feeds
- Coax cable connecting the CMM4 to the GPS antenna
- A patch cable between the Cluster Controller and the EtherWAN switch

3.2 POWER

The CMM4 requires a separately ordered 30-Volt AC-to-DC power supply. See Figure 4 for a picture of the power supply and Table 1 for part numbers.

IMPORTANT!
The power supply for the CMM4 must be separately ordered – it is not included when the CMM4 (1090CK) is ordered. This differs from the CMMmicro (1070CK), where the power supply is included when the CMMmicro is ordered.

On the DC side, the power supply has an attached 10 ft (3 m) DC cable with flying leads. On the AC side, the power supply has an IEC C14 chassis plug, commonly seen on electronic equipment such as computers and printers. The power supply is orderable with a North American IEC line cord or with no IEC line cord, in which case the operator must obtain the appropriate IEC line cord for their country.

The 30-Volt power supply is rated for outdoor temperatures, but is not weather tight and so must be mounted in a communications hut or enclosure provided by the operator. The 30-Volt power supply produces too much heat to be mounted inside the CMM4 enclosure.

Figure 4: 30 V Power Supply

Table 1: Power Supply Part Numbers

Name	Part Number
30 V Power Supply (North American 6 ft AC IEC line cord included)	ACPS112WA
30 V Power Supply (without AC line cord)	ACPS112W-02A

This same power supply is now included with CMMmicros (Cluster Management Module micro). Previously, Canopy has used 24-Volt DC power supplies, but all modules and radios are compatible with a 30 Volt system. The new Canopy 400 Series OFDM APs and SMs have higher power requirements and require a 30 Volt nominal system to ensure adequate power over the full range of supported Ethernet cable lengths and temperatures. For compatibility and simplicity, all power supplies for CMMs and SMs are moving to 30 Volts.

There are four input power terminal blocks inside the CMM4. Two of them are for 29/30 VDC input, and the other two are for 56 VDC input. The two 29 VDC terminal blocks allow the CMM4 to be powered from redundant power supplies, if so desired. The 56 VDC input power terminal blocks are currently unused and are reserved for future use.

Note, the CMM4 power supply is marked 30 VDC, the CMM4 is marked 29 VDC, and the latest SM power supplies are marked 29.5 VDC. All of these components are elements of a nominal 30 VDC system, and can be considered “30 VDC” elements.

The CMM4 cluster controller provides two 20 VDC outputs – one for the EtherWAN switch, and one optionally available for powering another low power device mounted in the enclosure by the operator, such as a fiber-to-copper media converter.

3.3 ARCHITECTURE

Figure 5 provides a diagram of the interior of the CMM4 enclosure. The cluster controller board of the CMM4 controls the application of power to the radios and inserts the GPS synchronization signal onto the Ethernet cable along with PoE. The cluster controller detects power faults and removes power from the faulted ports.

The controller must be connected to the Ethernet switch typically by cabling from the controller port to the Gigabit port.

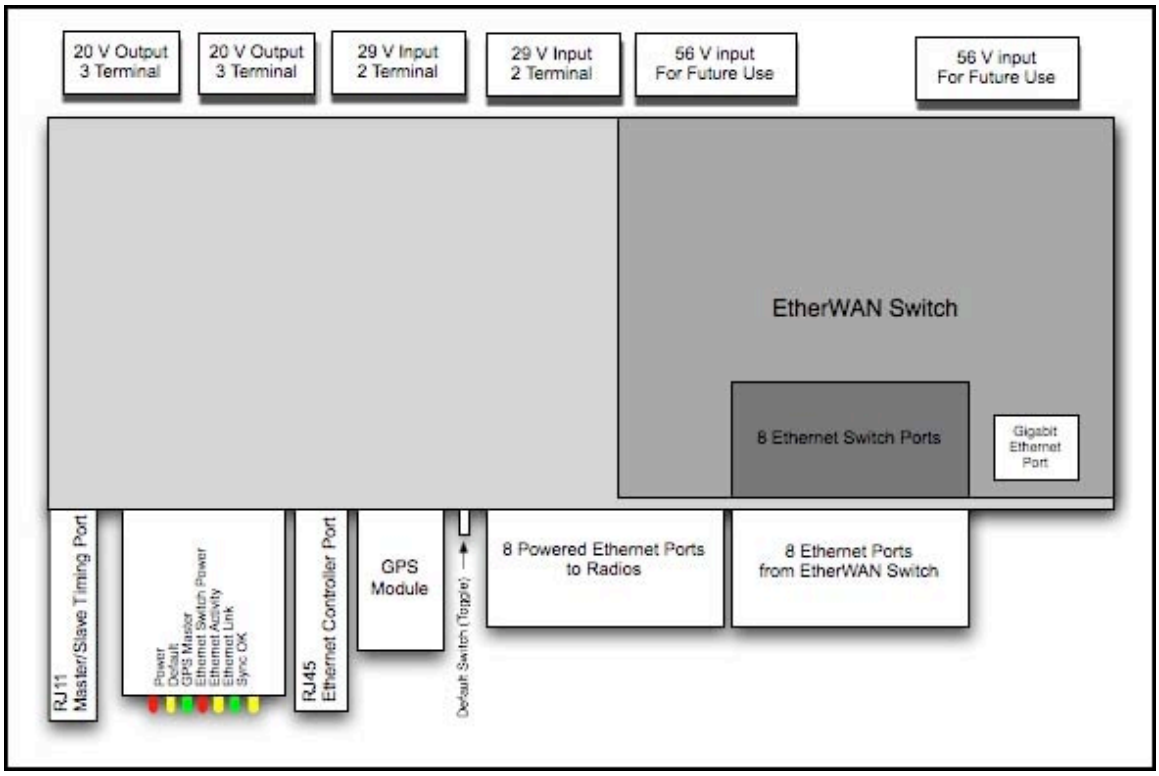


Figure 5: Diagram of CMM4 Components

Power over Ethernet for each port is independently controlled either from the web page or from SNMP. An on-board GPS module connects to the GPS antenna via coax cable and provides sync for the cluster controller to distribute as Sync over Power over Ethernet.

3.4 ETHERNET SWITCH

The Ethernet Switch is a 9-port hardened switch made by EtherWAN Systems and is mounted within the CMM4 enclosure. Eight ports support 10/100Base-T Ethernet and one port supports 1000Base-T (Gigabit) Ethernet. Typically, eight ports are connected to the eight ports on the cluster controller via eight Ethernet patch cables, and the ninth port is connected to the controller port of the cluster controller.

One of the ports on the switch must be cabled to the management port of the cluster controller (or other access to the controller must be provided). The eight Ethernet lines pass through the controller board and have power and sync injected, but do not

themselves provide network access to management of the controller board. If the Gigabit port isn't needed for Gigabit Ethernet, it is typically used for this purpose.

Switch management may be accessed in one of three ways:

- Administration console via the switch's RS-232 serial port.
  - This requires no IP address and is text-based using Windows Hyperterminal or equivalent.
  - Must be physically near the switch to access
- Web-based browser interface
  - Can be accessed from any location that has network access to the switch
- External SNMP-based network management application
  - Communicates with switch functions at the MIB level
  - Requires SNMP manager software or an Element Management System, such as Prizm.

The EtherWAN switch provides a full array of networking features. For information on features and configuration of the EtherWAN, see the *EtherWAN Switch Manual,* available for download at http://www.EtherWAN.com/manuals/es/EX96000_e1_Manual.pdf

3.5 SPECIFICATIONS AND LIMITATIONS

Table 2: CMM4 specifications and limitations

Specification or Limitation	System Range
Max length from CMM to any radio	328 cable feet (100 meters)
Max length from CMM to GPS antenna	100 cable feet (30.5 meters)
Max length from CMM to another CMM, if GPS sync cable is used	100 cable feet (30.5 meters)
Dimensions	20.75" x 14.75" x 7.75" (52.7 cm x 37.5 cm x 19.7)
Weight	14.0 lbs. (6.4 kg)
Operation Temperature	-40°F to +131°F (-40°C to +55°C)
Humidity	100% condensing
Ethernet, GPS Sync, and GPS Coax Cables	The use of cables that conform to the operational temperature of the product as well as being UV light protected is mandatory. Shielded Ethernet cables are strongly recommended

4 PLANNING

The following sections discuss planning for cabling and connectivity.

Information on the EtherWAN Switch, including planning information, is available in the *EtherWAN Switch Manual,* available for download at http://www.EtherWAN.com/manuals/es/EX96000_e1_Manual.pdf

4.1 TYPICAL LAYOUTS

Physical connectivity and cabling of the CMM4 is variable and is done per the specific requirements of a given installation. The following sections depict several variations for specific network configurations. Based on these typical layouts, operators should design connectivity and cabling that best meets their site-specific needs.

4.1.1 Standard Configuration

Figure 6 shows the CMM4's internal ports connected in a standard cabling configuration. In this configuration there are four Ethernet connections to Canopy radios and one connection to a terrestrial feed. The four Ethernet ports that are powered (indicated by a red light) were configured using the CMM4 configuration web page. The Ethernet connection to the terrestrial feed is not powered (no red light). An operator-provided Ethernet cable (not included) connects the cluster controller management port to the 1 Gbit interface on the EtherWAN switch. Ports 5, 6, and 7 are shown as unpowered and unused in this configuration. Local access during local maintenance could be gained by connecting an Ethernet cable from a local computer to any of the unpowered ports.

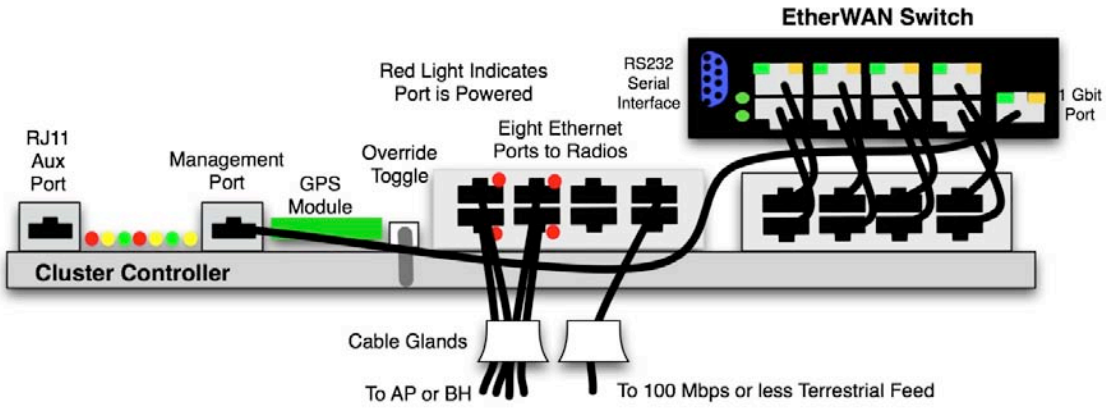


Figure 6: CMM4 Standard Configuration

CAUTION!

Do not mis-cable in such a way as to put power on the cluster controller management port.

4.1.2 Configured for 1000BaseT (Gigabit) Ethernet Terrestrial Feed

IMPORTANT!
The surge suppression provided by the cluster controller does not efficiently pass 1000BaseT (Gigabit) Ethernet. Connections required to support Gigabit Ethernet should not pass through the cluster controller portion of the CMM4 and should have separate surge suppression.

Figure 7 shows typical cabling for supporting a Gigabit Ethernet feed. The management port of the cluster controller is connected to port 7 and the Gigabit port of the EtherWAN switch is used for a terrestrial Gigabit Ethernet feed. The surge suppression on the cluster controller does not efficiently pass 1000BaseT (Gigabit) Ethernet, so the Gigabit Ethernet from the EtherWAN switch needs to

- Be cabled so as not to go through the cluster controller
- Have surge suppression provided using a Motorola PTP-LU Lightning Protection Unit. The PTP-LU should be mounted
  - within 3 ft (1 m) of the CMM4 if the CMM4 is located outdoors
  - on the outside of the building or communications hut at the point of cable entry if the CMM4 is located indoors.

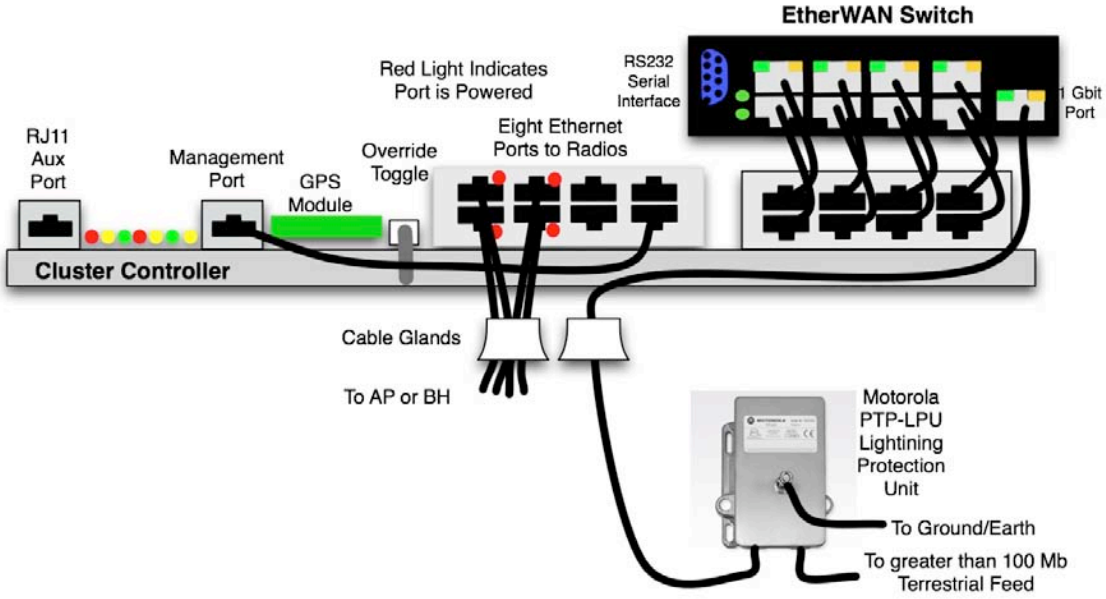


Figure 7: CMM4 cabled to use Gigabit Ethernet feed

4.1.3 Configured for PTP 400, 500, or 600 Series Ethernet Bridges

Motorola PTP 400, 500, and 600 Series Ethernet bridges can use the CMM4's EtherWAN switch for their network connectivity, as shown in Figure 8.

These units use a different powering scheme than Canopy units and must be powered using their external PIDU (Powered InDoor Unit), not the powering option of the cluster

controller in the CMM4. The PIDU must be located between the CMM4 and the ODU (OutDoor Unit – the radio), so as not to put power on ports of the EtherWAN switch.

IMPORTANT!
The surge suppression provided by the cluster controller does not efficiently pass 1000BaseT (Gigabit) Ethernet. Connections required to support Gigabit Ethernet should not pass through the cluster controller and should have separate surge suppression.

PTP 500 and PTP 600 Series bridges operate at greater than 100 Mbit speeds and so should not be cabled to the cluster controller portion of the CMM4. Surge suppression to protect the EtherWAN switch should be provided by a Motorola PTP-LU Lightning Protection Unit. The PTP-LU should be mounted

- within 3 ft (1 m) of the CMM4 if the CMM4 is located outdoors
- on the outside of the building or communications hut at the point of cable penetration if the CMM4 is located indoors.

PTP 400 Series bridges operate at less than 100 Mbit speeds and can be cabled to an unpowered port of the cluster controller, taking advantage of the cluster controller for surge suppression and being powered by their own externally located PIDU.

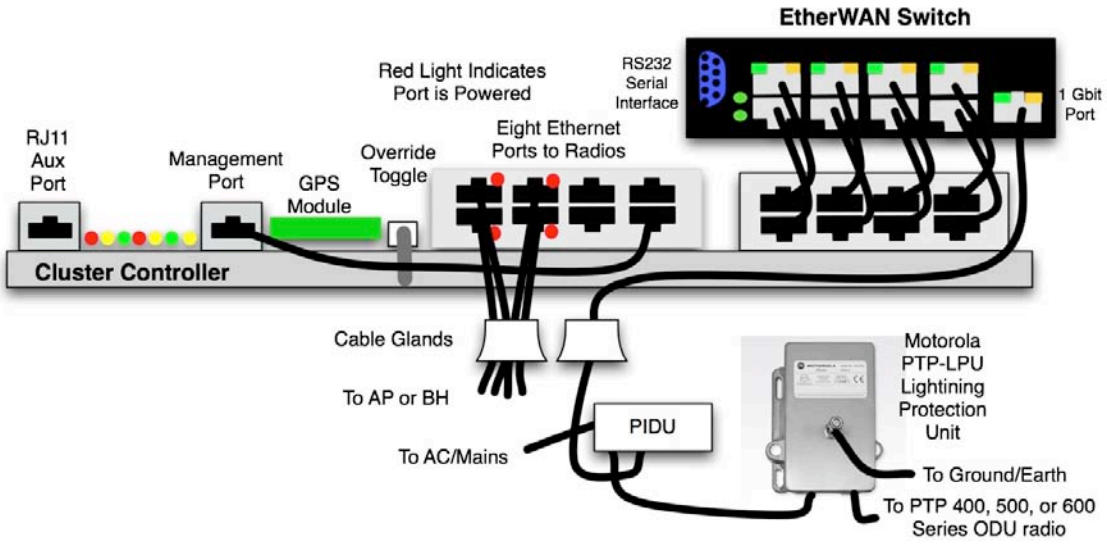


Figure 8: CMM4 cabled to support PTP 400/500/600

4.2 SYNCING TWO COLLOCATED CMMS TOGETHER

The auxiliary sync RJ-11 port can be used to connect two CMMs together to meet either of the following goals:

- Case 1 - Redundant Sync: Provide “warm spare” redundant sync when two CMMs are collocated, each with its own GPS antenna
- Case 2 – One GPS antenna for two CMMs: Use a single GPS antenna to support two CMMs.

The CMMs can be any combination of CMMs - either two CMM4s, two CMMmicros, or a CMM4 and a CMMmicro.

The connection cable is a special cable, not a straight-through cable. See section 4.3.3 for information on the cable and Figure 12 for cable pinouts. Figure 9 shows the cable connecting the RJ11 auxiliary port of a CMM to the RJ11 auxiliary port of a 2nd CMM.

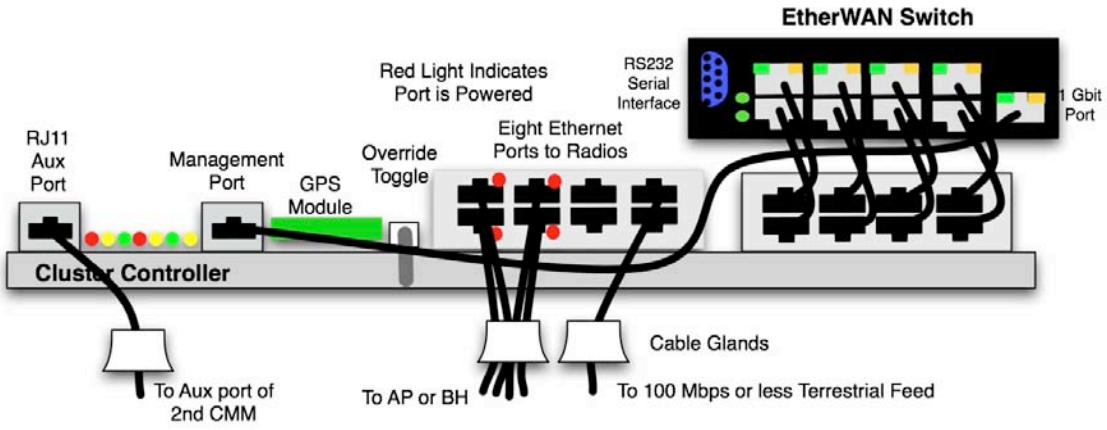


Figure 9: CMM4 cabled to support syncing another CMM

Case 1 – Redundant Sync

In this case, each CMM is connected to its own GPS antenna via coax in the standard way, and the two CMMs are connected via a special cable between the auxiliary sync RJ-11 ports of each CMM. If one CMM loses sync due to problems with its GPS antenna, coax cable, or GPS module, that CMM can be re-configured remotely over the network to get sync from the other CMM by going to the CMM => Configuration web page and setting the sync source to Slave (RJ11 Port).

In normal operation, the appropriate web pages of each CMM will display GPS information, as will the appropriate pages of connected APs and BHMs. Each CMM can be used as a NTP (Network Timing Protocol) server for time-of-day information for Canopy APs and BHMs, configured at the AP or BHM.

Once reconfigured to get sync over the auxiliary sync RJ-11 Port, a CMM and its connected APs and BHMs will no longer display GPS information. That CMM will no longer be providing NTP server functions, and any AP or BHM configured to point to it for

time-of-day will need to be re-configured to point to a different NTP server to get accurate time-of-day information.

Depending on network design and other equipment in the network, the two CMMs may be connected with an Ethernet cable, or may be each fed separately.

Case 2 – One GPS antenna for two CMMs

A typical scenario for the use of Case 2 would be where a site or building owner is charging per antenna, the site requires 2 CMMs, and the operator wishes to minimize site costs by only installing one GPS antenna.

In this case, the GPS antenna connects to one CMM via coax cable, and the two CMMs are connected via a cable between the auxiliary sync RJ11 ports of each CMM. Sync is passed from one CMM to the other via this cable. The Sync Source on the Configuration => CMM page of the CMM connected to the GPS antenna should be set to Master (GPS Module), and the Sync Source on the Configuration => CMM page of the other CMM should be set to Slave (RJ11 Port).

The slave CMM and its connected APs and BHMs will not display GPS information and the slave CMM will not function as an NTP (Network Time Protocol) server.

Depending on network design and other equipment in the network, the two CMMs may be connected with an Ethernet cable, or may be each fed separately.

4.3 CABLES

4.3.1 Ethernet Cables

The operator provides the Ethernet cables between the CMM4 and the radios it supports. They must be engineered to length and are not included with the CMM4.

In addition, the operator may need to provide an Ethernet cable connecting the management port of the cluster controller to the network. Options for this cable include

- A short 12-15 in (30-40 cm) operator-provided patch cable connecting the management port of the cluster controller to the Gigabit Ethernet port of the EtherWAN switch (this is the standard configuration, but only makes sense if the Gigabit Ethernet port isn't needed for Gigabit Ethernet use)
- A longer operator-provided cable connecting the management port of the cluster controller to the network via a collocated router or switch (this might be the preferred configuration if the CMM4 is located in a communications hut with other network gear, for example)
- Re-using one of the 12 in (30 cm) patch cables that comes connected between the EtherWAN switch and the cluster controller and instead using it to connect the management port of the cluster controller to the EtherWAN switch (this might be the preferred configuration if 7 or less of the Ethernet ports are needed for connecting to radios, thus freeing up one of the patch cables)

IMPORTANT!
The operator must provide network connectivity (a cable) to the management port of the cluster controller in order to be able to manager the cluster controller.

Although the cluster controller passes 8 Ethernet lines through it (providing protection and optionally sync and power), it does not provide any network connectivity for management of the cluster controller. Network connectivity must be provided by cabling the cluster controller management port to the EthernWAN switch or other network connection.

Cables are available from Best-Tronics, Inc., http://best-tronics.com/motorola.htm. These cables can be ordered in lengths up to 328 ft (100 m) and are listed in Table 3.

Table 3: Recommended Ethernet Cables

Typical Use	Best-Tronics Part #	Description
Infrastructure Ethernet cable	BT-0781S-XXX	RJ-45 to RJ-45 straight, shielded, UV-resistant Ethernet cable using outdoor STP Cat 5e cable, lower cost than plenum-rated, available only in black.
Infrastructure Ethernet cable for plenums	BT-0562S-XXX	RJ-45 to RJ-45 straight, shielded, UV-resistant, plenum-rated Ethernet cable using outdoor STP Cat 5e cable, available in beige, blue, grey, or white.

IMPORTANT!
Shielded Ethernet cable is strongly recommended for AP and BH installations.

Alternatively, equivalent cables may be procured by the operator, fabricated by the operator in a depot, or fabricated at site. The modules have auto MDX/MDIX and so either straight-through or crossover Ethernet cables may be used. Pinouts for straight-through cables are shown in Figure 10. Figure 11 shows the location of Pin 1, relative to the lock tab on the connector.

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.

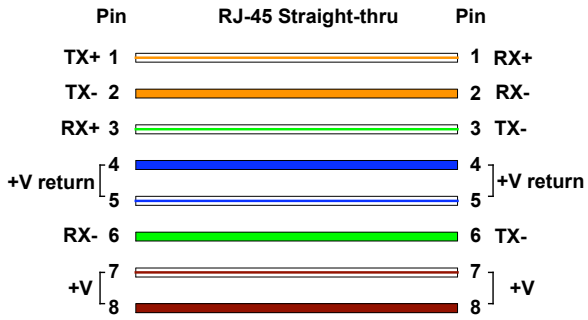


Figure 10: RJ-45 pinouts for straight-through Ethernet cable

(Lock tab underneath)

Figure 11: Location of Pin 1

Bulk unterminated Ethernet cable can be ordered from Best-Tronics as bulk cable:

CA-0287S: (shielded, plenum rated)

CA-0367S: (lower cost, shielded, non-plenum-rated)

4.3.2 GPS Antenna Coaxial Cable

The operator provides the GPS antenna coaxial cable between the CMM4 and the GPS antenna. It must be engineered to length and is not included with the CMM4.

Antenna cables can be ordered from Best-Tronics, Inc., http://best-tronics.com/motorola.htm. Antenna cables can be ordered in lengths up to 100 ft (30.4 m), as listed in Table 4.

Table 4: Recommended Antenna Cable

Best-Tronics Part #	Description
BT-0564	N to N GPS antenna cable

Alternatively, equivalent cables may be procured by the operator, fabricated by the operator in a depot, or fabricated at site using

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

NOTE:
The CMM4 has a female N-type coax connector on the outside of the enclosure, whereas the CMMmicro has a female BNC-type connector inside the enclosure. Take this into account when ordering or fabricating cables, and when replacing a CMMmicro with a CMM4.

4.3.3 CMM Sync Cable

Two CMMs (two CMMmicros, two CMM4s, or a CMMmicro and a CMM4) can be connected together with a CMM sync cable to provide either

- "Warm spare" redundant sync
- The ability to have one GPS antenna support two CMMs

When this option is desired, a special cable must be fabricated. Pinouts for this cable are shown in Figure 12. Figure 11 shows the location of Pin 1, relative to the lock tab on the connector.

NOTE:
The CMM sync cable used to connect two CMMs together has different pinouts than the straight through sync cable used to connect an SM to a "remote AP" or to connect an AP or BH to a CMM2.

Pin 1 → white / orange ← Pin 2
Pin 2 → white / green ← Pin 1
Pin 3 → open ← Pin 3
Pin 4 → open ← Pin 4
Pin 5 → green ← Pin 6
Pin 6 → orange ← Pin 5

NOTE: The third and fourth pairs are not used.

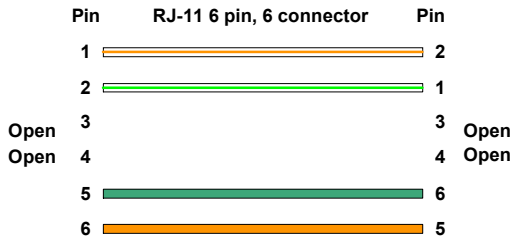


Figure 12: CMM sync cable pinouts

4.3.4 Category 5 Ethernet Cable Tester

For purchase within the U.S.A., the CTCAT5-01 Cable Tester is available.

5 CONFIGURING A CMM4

Web pages on the CMM4 provide status information and support configuration. The eight Ethernet ports can be configured, and information is provided on GPS status, Port configuration, FPGA and software revision.

For information on configuring the EtherWAN switch, see the *EtherWAN Switch Manual.* The manual comes on a CD with the CMM4, and is also available for download at http://www.EtherWAN.com/manuals/es/EX96000_e1_Manual.pdf

5.1 LOG IN

An example of the CMM4 Login page is displayed in Figure 13.

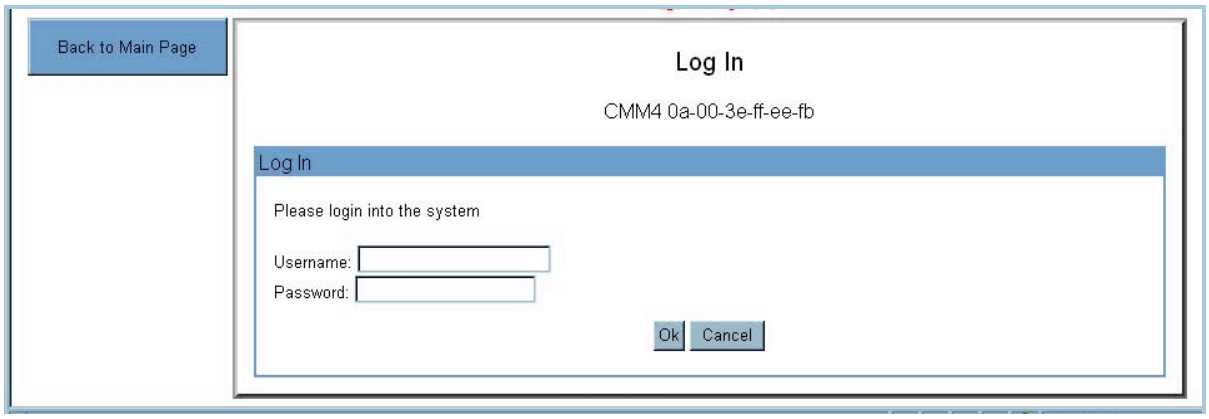


Figure 13: Login Page of CMM4, Example

To access the web pages of the CMM4 as a user whose level is above GUEST, you must use the Login page to enter a user name and password that have been provisioned for the higher level.

The left side of the web page displays the current user name as **Account** and the permissions level of that user as **Level**. If you are already logged in and want to log in now as a different user, use the following sequence:

- On the left side of the web page, click **Logoff**.

Navigate or proxy once again to the Home page of the CMM4.

On the left side of the web page, click **Login**.

Use the Login page as described above.

When you are logged in, you have no further access to the Login page, other than by this sequence.

5.2 VIEWING GENERAL STATUS

An example of the CMM4 General Status tab is displayed in Figure 14.

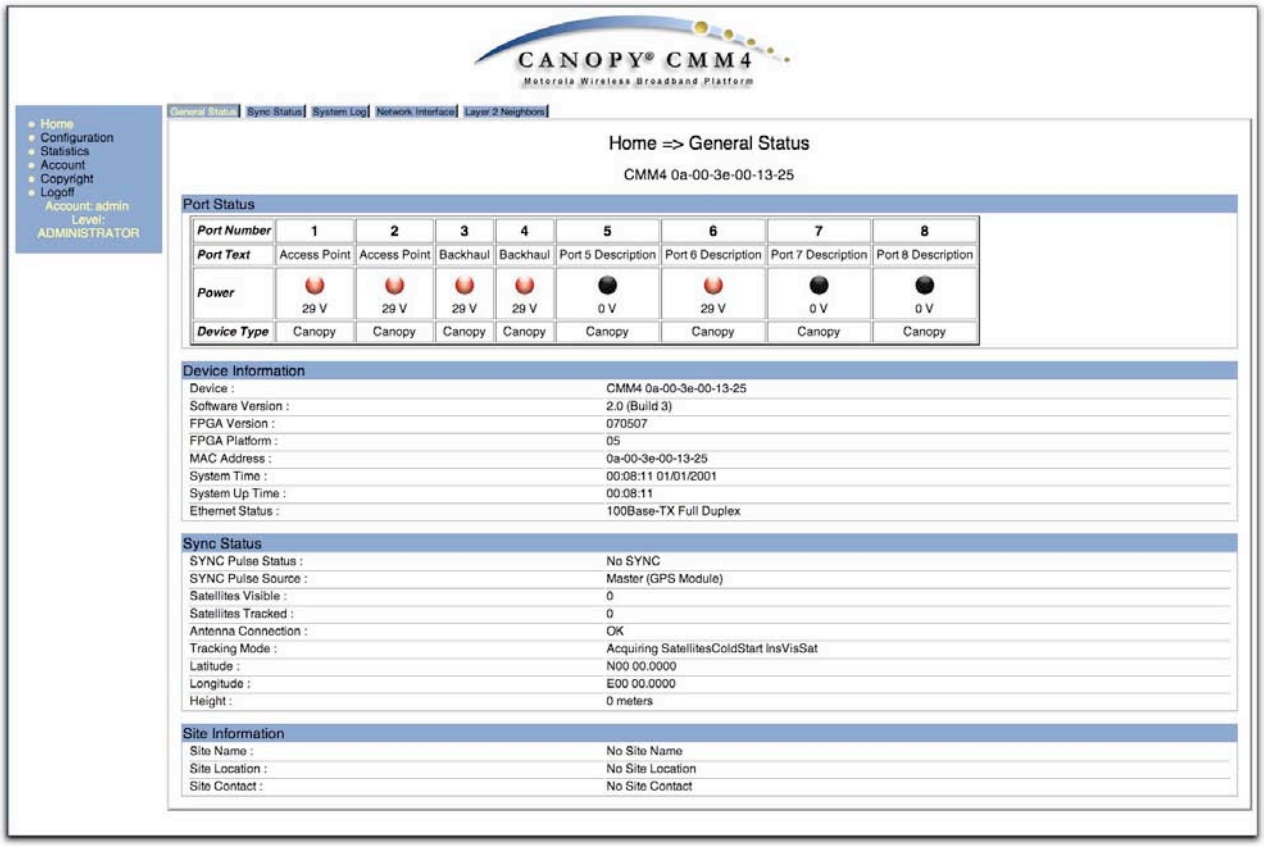


Figure 14: General Status Tab of CMM4, Example

The General Status tab provides information on the operation of the CMM4. This is the tab that opens by default when you access the GUI. The General Status tab provides the following read-only fields.

Device

This field indicates the type of the Canopy module and provides its MAC address.

Software Version

This field indicates the CMM4 release and the time and date of the release. If you request technical support, provide the information from this field.

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.

FPGA Platform

This field indicates the hardware platform that the FPGA runs on.

MAC Address

This field displays the MAC address (or electronic serial number) of the CMM4.

System Time

This field provides GMT (Greenwich Mean Time) and date to all connected devices, which they in turn pass to devices that register to them. Data for this field is from the GPS device.

System Up Time

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

Ethernet Status

This field indicates the speed and duplex state of the Ethernet interface to the CMM4.

SYNC Pulse Status

This field indicates the status of synchronization as follows:

- **SYNC OK** indicates that the module is receiving the sync pulse.
- **No SYNC** indicates that the module is set to receive a sync pulse from an outside source and is not receiving the pulse.

SYNC Pulse Source

The GPS device, from another CMM4 master, or from an AP, may generate sync.

Satellites Visible

This field displays the number of satellites whose signals are received by the connected GPS antenna.

Satellites Tracked

This field displays the number of satellites whose signals the CMM4 uses.

Antenna Connection

This field indicates the health of the connection between the CMM4 and the GPS antenna.

Tracking Mode

If the CMM4 receives the signals from a GPS antenna, then this field describes the degree to which the CMM4 is accurately computing position information, given the satellites that it is tracking.

Latitude

If the CMM4 receives the signal from a GPS antenna, then this field displays the latitude of the site.

Longitude

If the CMM4 receives the signal from a GPS antenna, then this field displays the longitude of the site.

Height

If the CMM4 receives the signal from a GPS antenna, then this field displays the elevation (above sea level) of the GPS antenna.

Site Name

This field indicates the name of the physical module. You can assign or change this name in the SNMP tab of the CMM4 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 CMM4 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 CMM4 Configuration page. This information is also set into the *sysName* SNMP MIB-II object and can be polled by an SNMP management server.

5.3 VIEWING SYNC STATUS

An example of the CMM4 Sync Status tab is displayed in Figure 15.

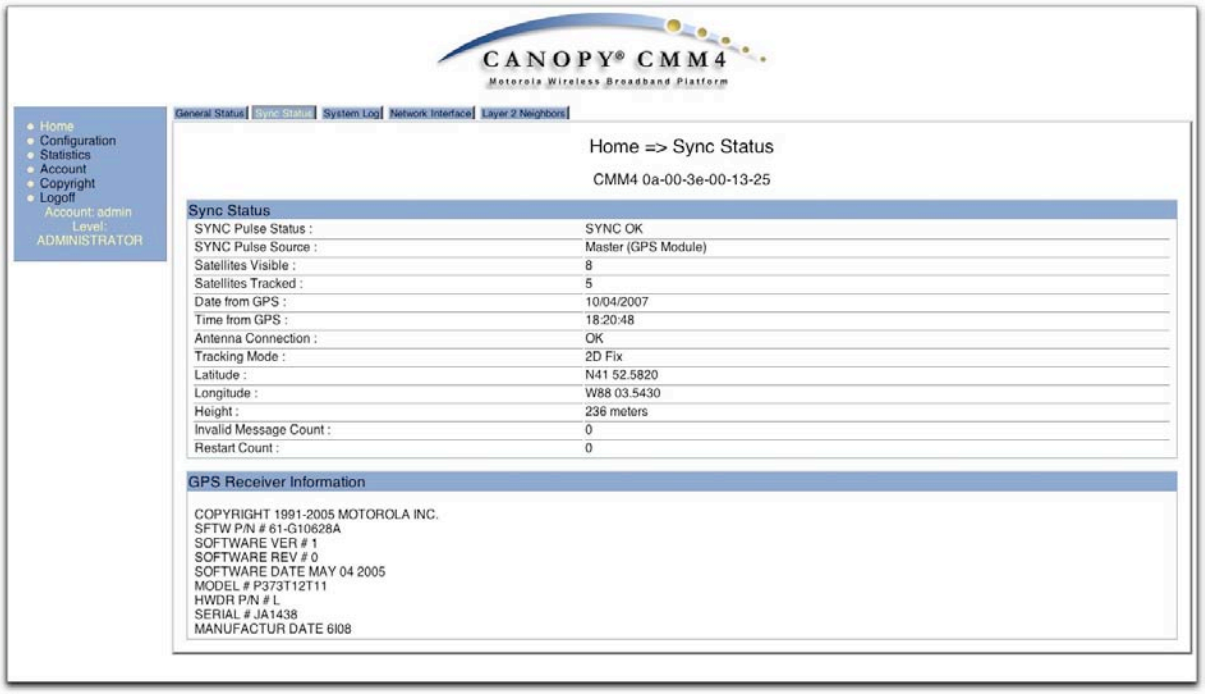


Figure 15: Sync Status Tab of CMM4, Example

The Sync Status tab provides information on the GPS receiver in this CMM4 and the signals that it is receiving.

SYNC Pulse Status

This field indicates the status of synchronization as follows:

- **SYNC OK** indicates that the module is receiving a sync pulse from an outside source and is receiving the pulse.
- **No SYNC** indicates that the module is set to *receive* a sync pulse from an outside source and is not receiving the pulse.

Satellites Visible

This field displays the number of satellites from which the connected GPS antenna receives a signal.

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

Satellite Tracked

This field displays the number of satellites whose signals the CMM4 uses.

Date from GPS

This field displays the month, day, and year that the CMM4 receives.

Time from GPS

This field displays the hour, minute, and second that the CMM4 receives.

Antenna Connection

This field indicates the health of the connection between the CMM4 and the GPS antenna.

Tracking Mode

If the CMM4 receives the signals from a GPS antenna, then this field indicates the degree to which the CMM4 is accurately computing position information, given the satellites that it is tracking. For example

- `2D Fix` indicates that the CMM4 has a lock on information that is sufficient to compute position.
- `Bad Geometry` indicates that it does not.

Latitude

If the CMM4 receives the signal from a GPS antenna, then this field displays the latitude of the site.

Longitude

If the CMM4 receives the signal from a GPS antenna, then this field displays the longitude of the site.

Height

If the CMM4 receives the signal from a GPS antenna, then this field displays the elevation (above sea level) of the GPS antenna.

Invalid Message Count

Number of messages sent from the GPS receiver for which there is no match.

Restart Count

It is incremented when the CMM4 is having difficulty communicating with the GPS module.

5.4 VIEWING THE SYSTEM LOG

An example of the CMM4 System Log tab is displayed in Figure 16.

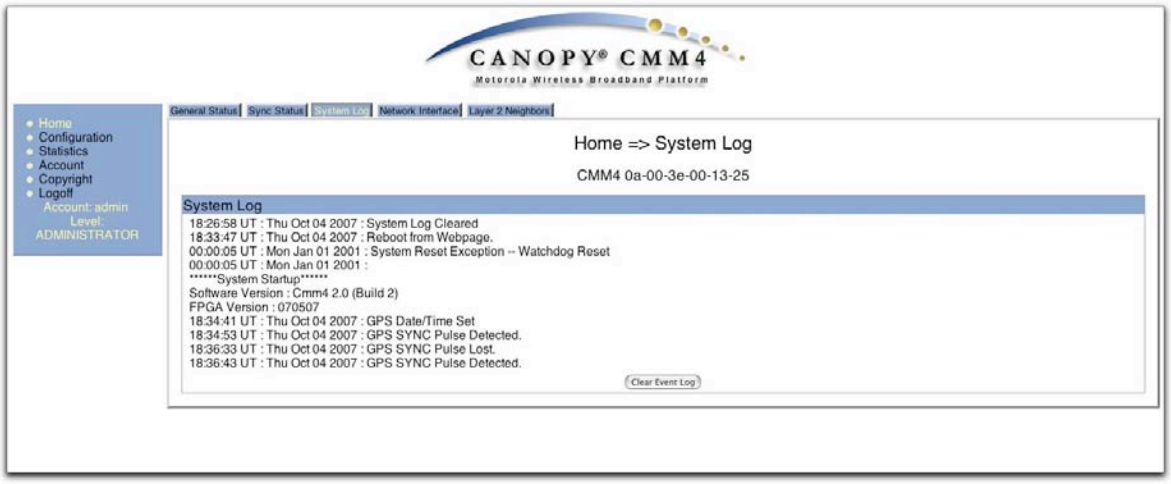


Figure 16: System Log tab of CMM4, Example

The System Log tab provides a record of events that have been significant to this CMM4.

5.5 VIEWING THE NETWORK INTERFACE

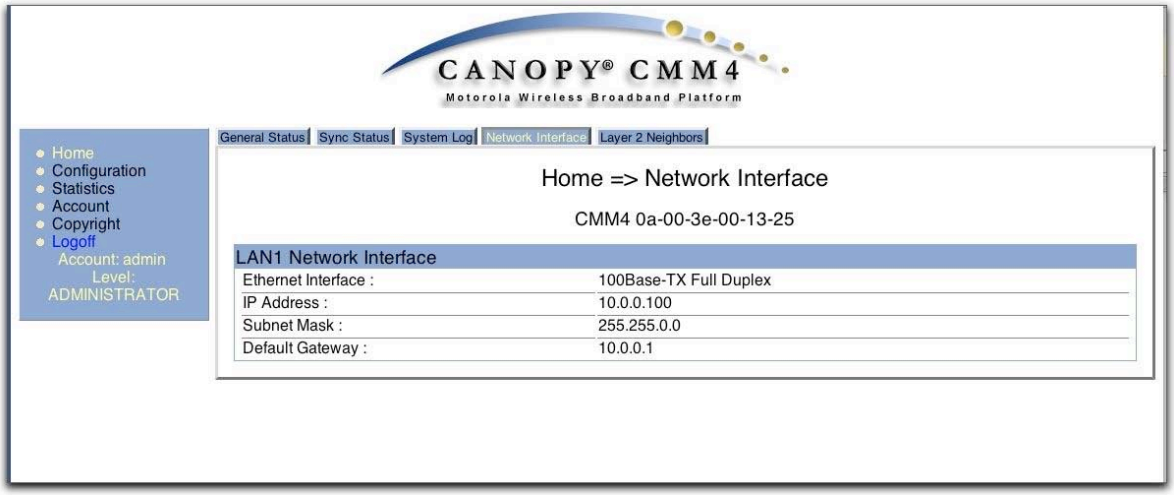


Figure 17: Network Interface, Example

The Network Interface screen allows the operator to view the LAN settings for the CMM4 device. It is a read-only screen.

Ethernet Interface

This field displays the Ethernet mode of the LAN port.

IP Address

This field displays the IP address that the operator has set for the CMM4 cluster controller. This field is set in the CMM4 Configuration tab. The Ethernet Switch has a separate IP address.

Subnet Mask

This field displays the address of the subnet mask. Subnetting allows the network to be logically divided without regard to the physical layout of the network.

Default Gateway

This field displays the address of the default gateway. A default gateway is a node on the network that serves as an access point to another network.

5.6 VIEWING LAYER 2 NEIGHBORS

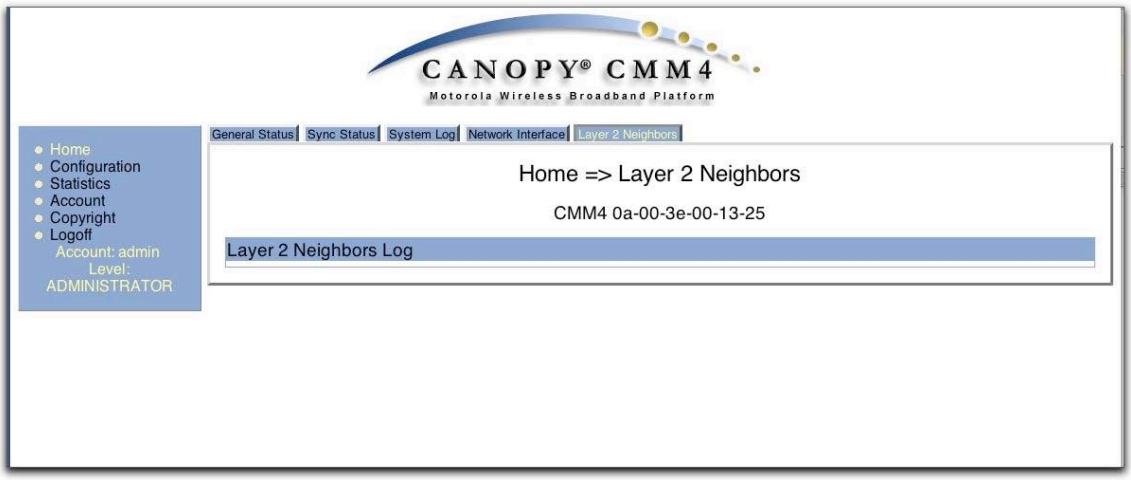


Figure 18: Layer 2 Neighbor Table, Example

This screen provides information on all of the layer 2 devices communicating with the CMM4 including any Canopy devices on an Ethernet connected hub.

5.7 CONFIGURATION

An example of the CMM4 Configuration tab is displayed in Figure 19.

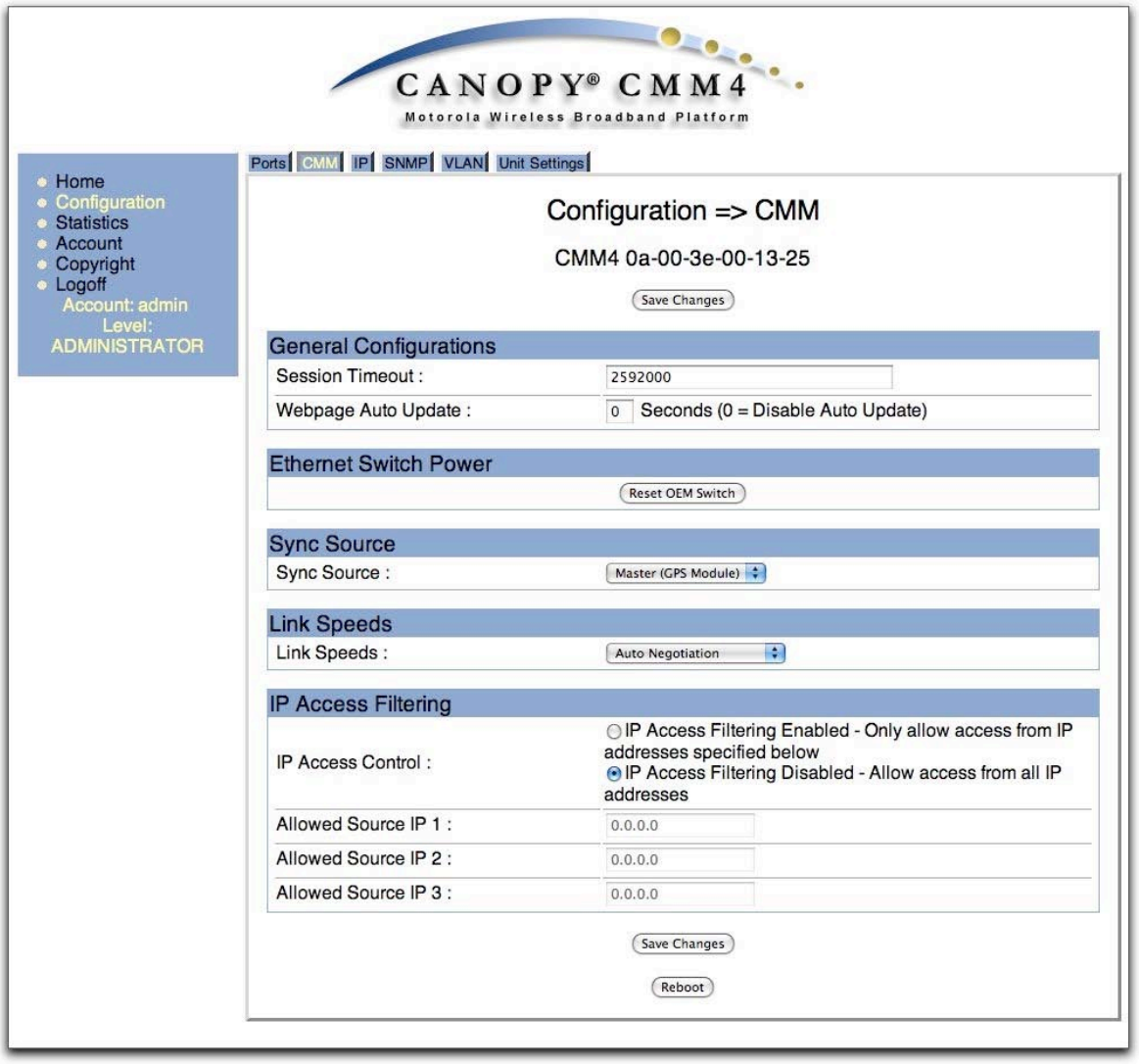


Figure 19: CMM4 Configuration Tab of CMM4, Example

The CMM4 Configuration tab provides the following parameters.

Session Timeout

Enter the expiry in seconds for remote management sessions via HTTP, telnet, or ftp access to the CMM4 up to a maximum of 2592000 seconds.

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**, the change becomes effective immediately and the previous value is lost.

Reset Ethernet Switch

This reboots the Ethernet Switch. It may be used if you lose your userid or password and need to override the current settings. Following is a procedure for resetting your userid or password on the Switch.

Procedure 1: Reset Ethernet Switch Userid or Password

========== **Start of procedure** ==========

1. Connect the RS-232 serial port to a Windows PC using the included serial cable.
2. Open a HyperTerminal using settings of 115200 8-N-1 in VT100. To find and open Hyperterminal, go to Help, enter Hyperterminal, and follow directions for your Windows operating system.
3. Reboot the EtherWAN Switch, either by power cycling the entire CMM4, or using the "Reset OEM Switch" button on the CMM4 Controller GUI.
4. Press "Esc" to enter boot prompt
5. Press "ctrl"+"d" to get to DBG prompt
6. Type "read -b 1ffe08020 100"
7. The password is shown on the right hand side of the first row.

========== **End of procedure** ==========

Sync Source

Specify how the CMM4 should receive timing, either

- **Master (GPS Module)**
- **Slave (RJ11 Port)**

Link Speeds

If you wish to force the CMM4 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 is defined in Table 5.

Table 5: Link Speed selections for CMM4

Selection	Result
Auto Negotiation	The CMM4 attempts to auto-negotiate speed and duplex state. (This is the default and recommended setting.)
10Base T Half Duplex	The CMM4 is forced to 10 Mbps and half duplex.
10Base T Full Duplex	The CMM4 is forced to 10 Mbps and full duplex.
100Base T Half Duplex	The CMM4 is forced to 100 Mbps and half duplex.
100Base T Full Duplex	The CMM4 is forced to 100 Mbps and full duplex.

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

IP Access Control

You can permit access to the CMM4 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 CMM4 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.

5.8 SETTING THE IP COMMUNICATIONS PARAMETER

An example of the CMM4 IP tab is displayed in Figure 20.

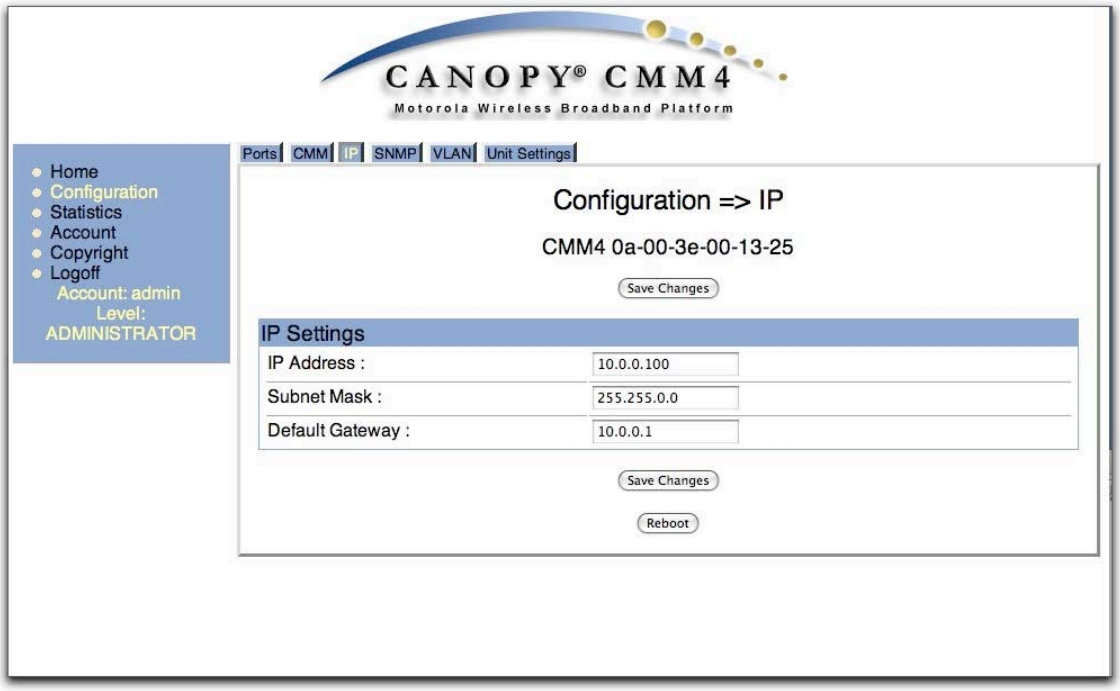


Figure 20: IP tab of CMM4, Example

The IP tab allows you to set the IP communications parameter for management of the CMM4.

IP Address

This is the IP address of the CMM4 (Cluster Controller). The Ethernet Switch has a separate and distinct IP address that is set using the Ethernet Switch web interface.

Subnet Mask

This is the subnet mask of the CMM4 (Cluster Controller). The Ethernet Switch has a separate subnet mask that is set using the Ethernet Switch web interface.

5.8.1 Overriding Forgotten IP Addresses or Passwords on CMM4

By using an override toggle switch on the CMM4 circuit board, you can temporarily override a lost or unknown IP address or password as follows:

- The override position of the toggle is up in which a power cycle causes the CMM4 to boot with the default IP address (169.254.1.1) and no password required.
- The normal position of the toggle is down in which a power cycle causes the CMM4 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 2: Using the override switch to regain access to CMM4

========== **Start of procedure** ==========

IMPORTANT!

In override mode a CMM4 provides no power on its ports, so no APs or BHs connected to the CMM4 will be powered, and you will not be able to access the CMM4 through any connected APs or BHs.

If you reboot without the default switch, the ports will return to the state they were in before the override. Those that were powered before will be powered again. However, if you click "Save Changes" on the Configuration->Ports page before rebooting then this new configuration will be saved to flash, and the next boot will come up with the new port configuration.

1. Gain physical access to the inside of the CMM4 enclosure.
2. Establish direct Ethernet connectivity to the CMM4 (not through an AP or BH).
3. Flip the toggle switch up (toward you).
4. Power cycle the CMM4.
   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** ==========

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.

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.

5.9 CONFIGURING THE CMM4 PORTS

An example of the CMM4 Port Configurations tab is displayed in Figure 21.

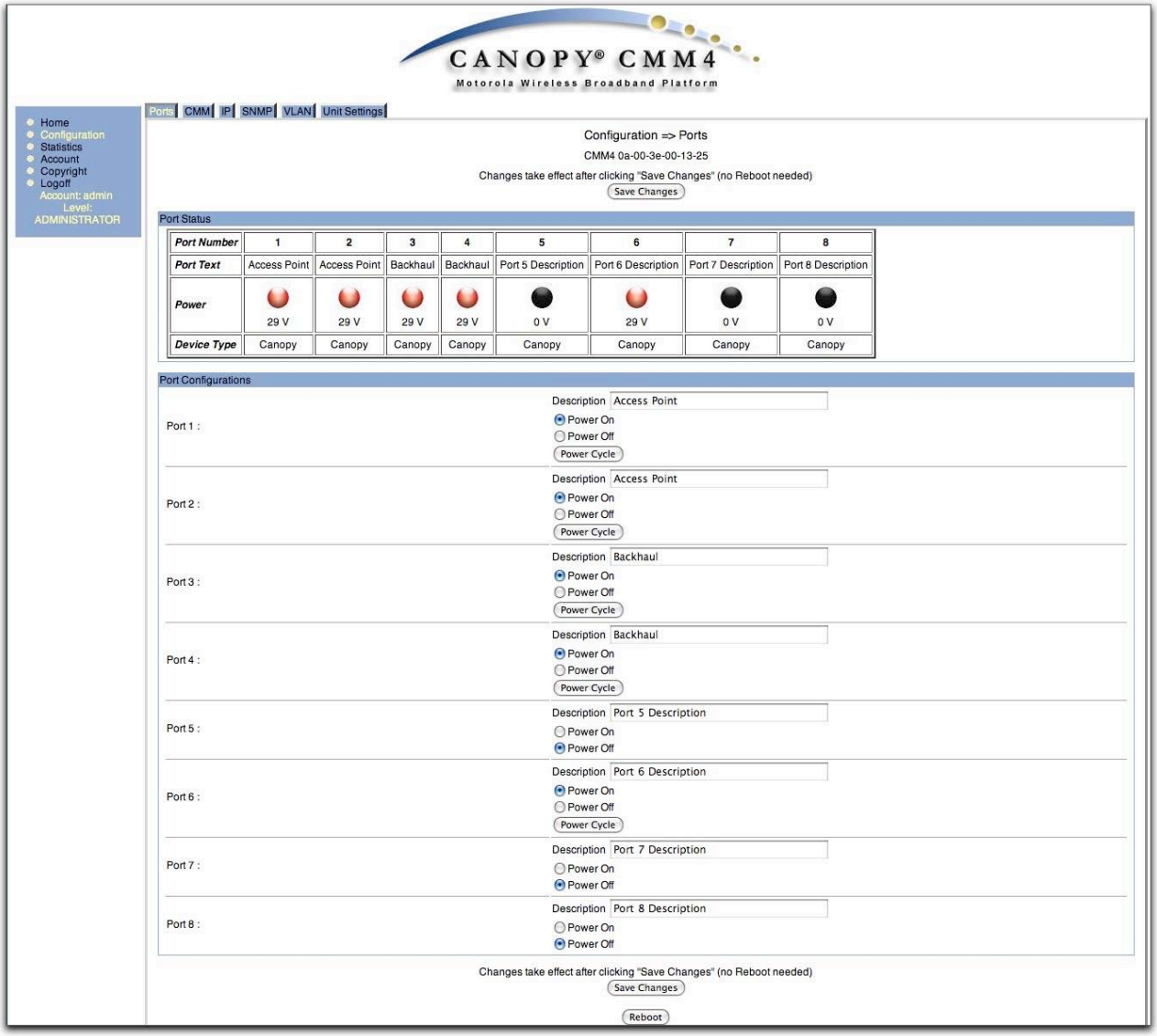


Figure 21: Port Configurations tab of CMM4, Example

The Port Configurations tab provides the following parameters.

Port *1 to 8*: Description

This is a user-defined field that identifies the port. It appears in the Home -> General Status page.

Port *1 to 8*: Power *On or Off*

Select **Power On** to restore power over Ethernet to the device that is connected to this port or **Power Off** to remove power from it.

Ports *1 to 8*: Power Cycle

A button to invoke this feature is visible only when the port is powered up.

Save Changes

The port power configuration changes take place immediately upon selecting “Save Changes.”

Reboot

This can be used to reboot the unit at any time.

5.10 CONFIGURING THE SNMP PARAMETERS

An example of the CMM4 SNMP tab is displayed in Figure 22.

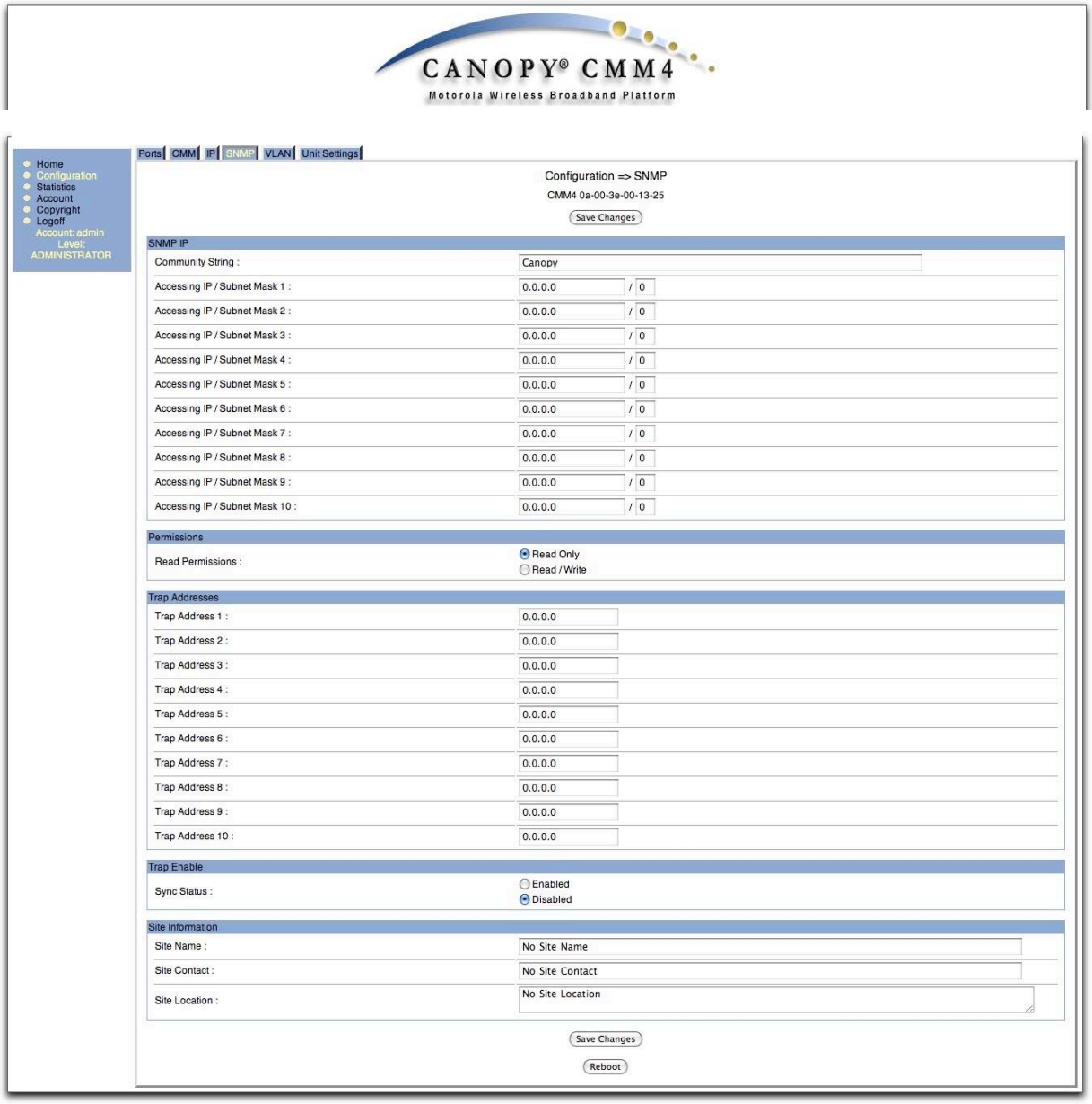


Figure 22: SNMP tab of CMM4, Example

The SNMP tab provides the following parameters.

Community String

Specify a control string that allows Prizm or a Network Management Station (NMS) to access the CMM4 via SNMP. No spaces are allowed in this string. The default string is **Canopy**. The value is clear text and is readable by a packet monitor. You can attain

additional security by configuring the **Accessing Subnet** and **Read Permissions** parameters.

Accessing Subnet

Specify the addresses that are allowed to send SNMP requests to this CMM4. 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 CMM4, presuming that the device supplies the correct **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.

Read Permissions

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

Trap Address *1 to 10*

Specify the IP address (xxx.xxx.xxx.xxx) of one to ten servers (Prizm or NMS) to which trap information should be sent. Traps inform 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.

Trap Enable for Sync Status

Variable to enable/disable GPS sync/out-sync traps.

Site Name

Enter a name for the physical module. What you enter here will be shown on the General Status tab in the Home page of the CMM4. This information is also set into the *sysName* SNMP MIB-II object and can be polled by an SNMP management server.

Site Contact

Enter contact information for the physical module. What you enter here will be shown on the General Status tab in the Home page of the CMM4. This information is also set into the *sysName* SNMP MIB-II object and can be polled by an SNMP management server.

Site Location

Enter site information for the physical module. What you enter here will be shown on the General Status tab in the Home page of the CMM4.

5.11 CONFIGURING VLAN

An example of the CMM4 VLAN tab is displayed in Figure 23.

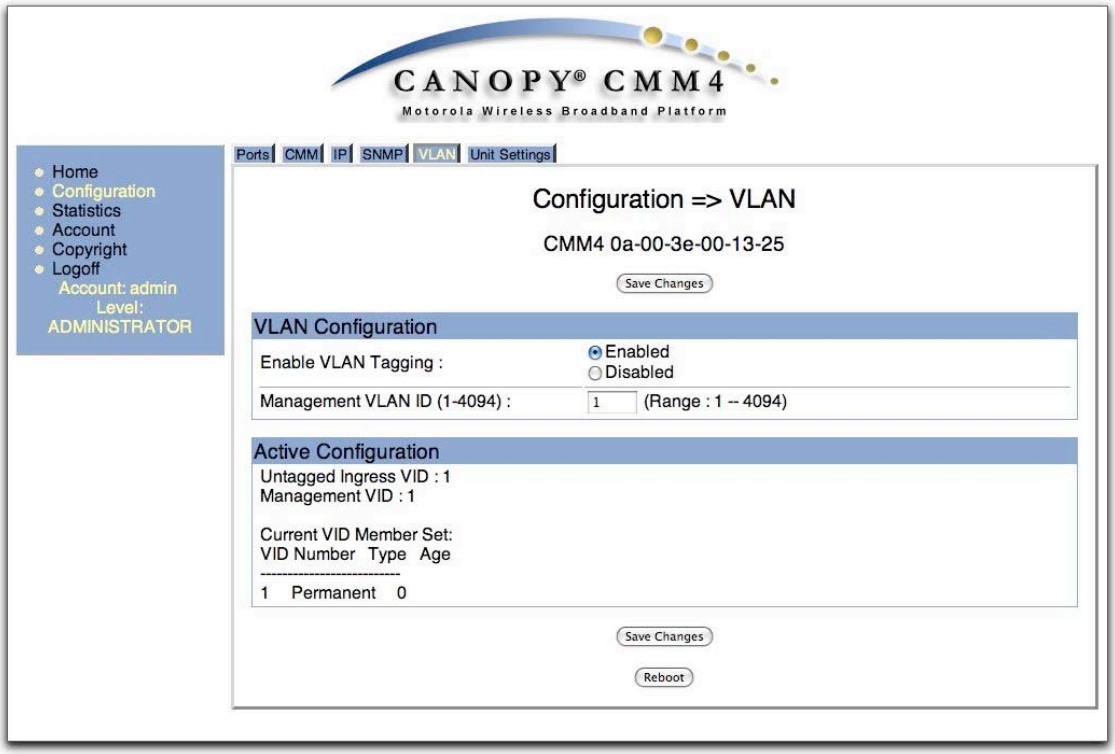


Figure 23: VLAN tab of CMM4, Example

The VLAN tab provides the following parameters.

Enable VLAN Tagging

If this parameter is set to **Enabled** and a **Management VLAN ID** is set in the next parameter, then the management controller of the CMM4 will accept only frames that are

VLAN tagged with the configured tag value. All frames outgoing from the management controller of the CMM4 will have a VLAN tag, set to the configured VLAN ID.

Management VLAN ID

If **Enable VLAN Tagging** is set to **Enabled** and this parameter is set, then the management controller of the CMM4 will accept only frames that are VLAN tagged with the configured tag value. All frames outgoing from the management controller of the CMM4 will have a VLAN tag, set to the configured **Management VLAN ID**.

Active Configuration

This field indicates the status of the current configuration. For example, VLAN tagging enabled with "1" set as the management VLAN tag would display the following:

Untagged Ingress VID: 1

Management VID: 1

Current VID Member Set:

VID Number	Type	Age
1	Permanent	0

Note that Management VLAN "1" has special properties that allow untagged VLAN frames to communicate with the device (CMM4 or radio). If the Management VLAN ID is set to 1 the local stack of the unit will accept VLAN 1 or untagged. If the Management VLAN is set to anything but 1, it will only allow that specific VLAN tag to enter the stack; it will not accept untagged frames.

5.12 CONFIGURING THE UNIT SETTINGS

An example of the CMM4 Unit Settings tab is displayed in Figure 24.

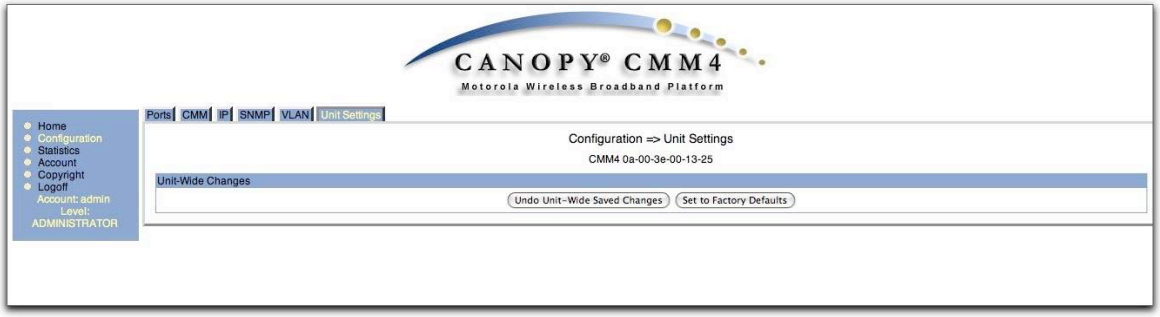


Figure 24: Unit Settings Tab of CMM4, Example

The Unit Settings tab provides the following buttons.

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.

5.13 VIEWING THE ARP TABLE (STATISTICS)

Figure 25 displays read-only information on the Address Resolution (ARP) table. This ARP table provides information on the data devices connected to the CMM4. The ARP Table maps the IP address to the MAC address. The table also shows the age of the entry in the table, the interface (in this case it will always be Ethernet "et1"), and whether the packets are "pending."

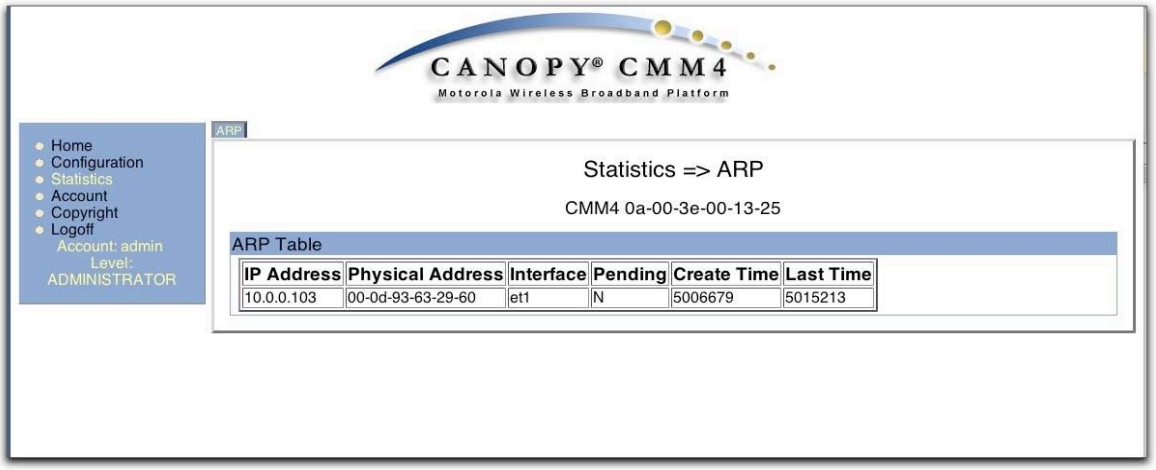


Figure 25: ARP Table, Example

This ARP table example displays information on the laptop computer attached to the CMM4 for the purpose of Internet access.

IP Address

This field displays the IP address of the device connected to the CMM4.

Physical Address

This field displays the machine address of the device connected to the CMM4. A physical address cannot be changed. The ARP table is used by the system to translate the logical address into a physical address.

Interface

This field displays the type of interface. In the case of the CMM4, the interface will always be an Ethernet interface.

Pending

This field indicates whether the packets are pending "Y" or "N."

Create Time/Last Time

These fields are used to “age out” the entry in the table in the case where there has been no communication for a period of time.

5.14 USER UPDATE

An example of the CMM4 User Update tab is displayed in Figure 26.

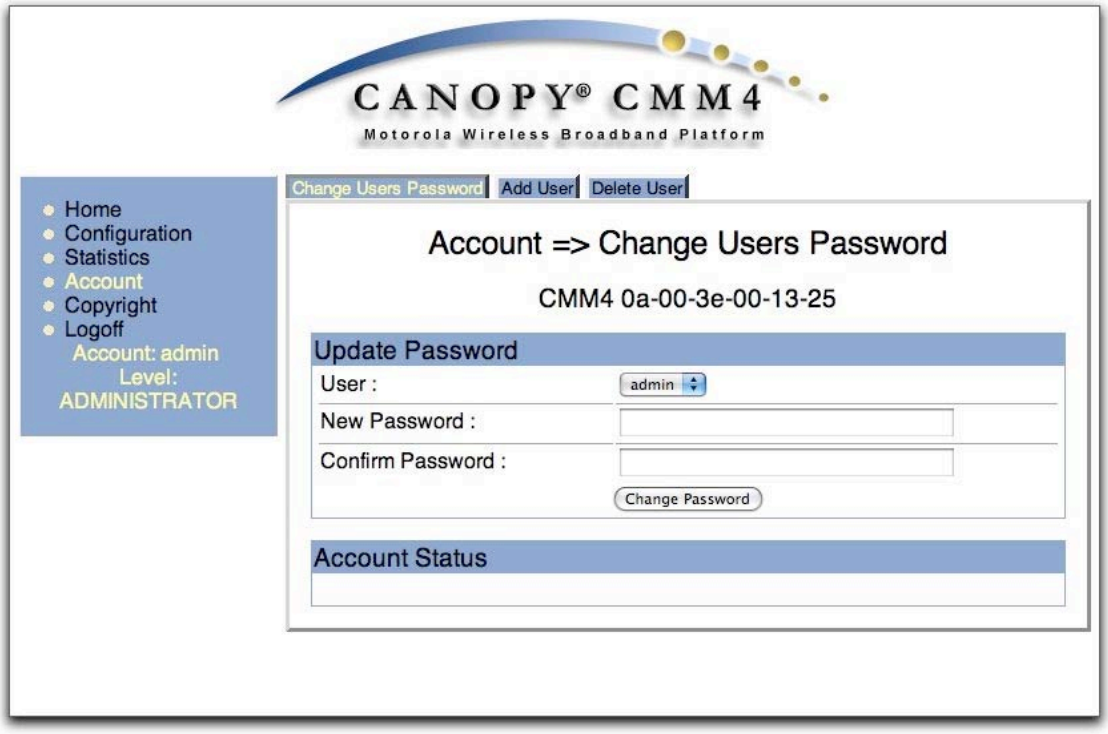


Figure 26: Change Users Password Tab of CMM4, Example

The Change Users Password tab provides the following options:

New Password

Type the new password (up to 32 alphanumeric characters) that you want to use for management access to this CMM4.

Confirm Password

Retype what you typed into the **New Password** parameter. If the password differs from the password you typed into the **New Password** field a failure message will be displayed in the **Account Status** field.

Change Password

To put the new password for the user into immediate effect, click this button.

Account Status

This is a read-only field that provides information on the current activity for that screen. For instance, if changing the password was successful a message will be displayed

indicating the new password is active.

5.15 ADD USER

An example of the CMM4 Add User tab is displayed in Figure 27.

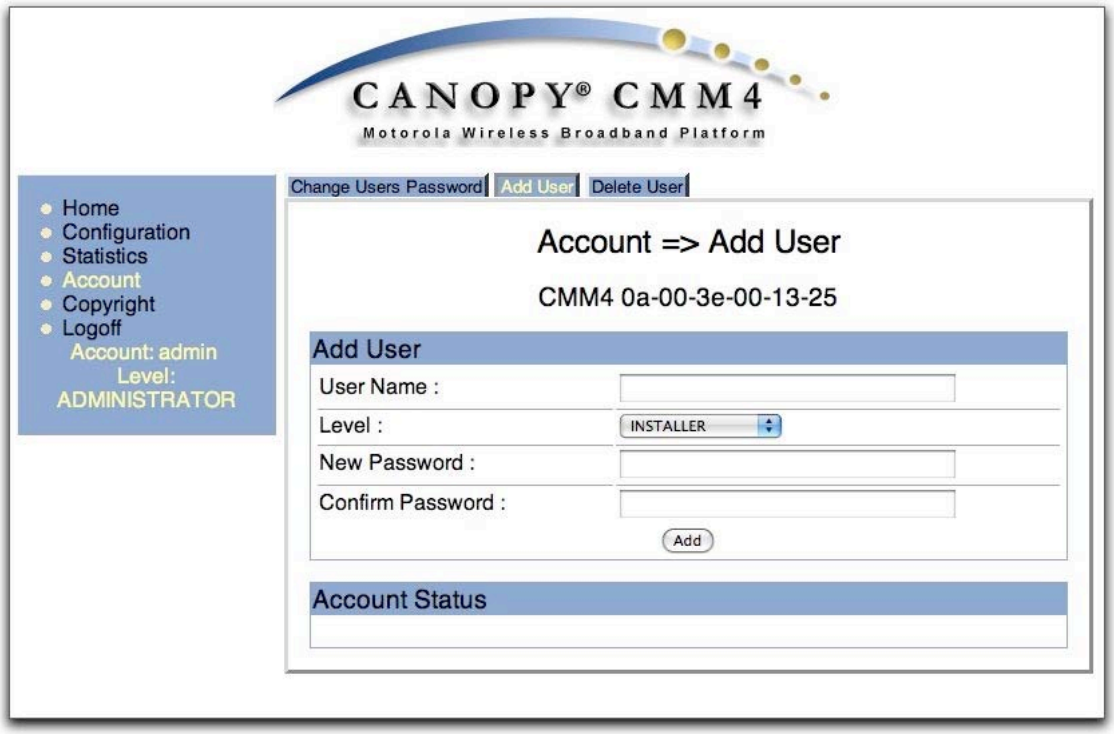


Figure 27: Add User Tab of CMM4, Example

If you are of ADMINISTRATOR level and want to add a user, the Add User Tab provides the following options to you.

User Name

Type the user name that you want to assign to the user you are adding.

Level

Use the down arrow to select the desired permissions level for the user you are adding.

New Password

Type the new password (up to 32 alphanumeric characters) for management access to this CMM4 by the user you are adding.

Confirm Password

Retype what you typed into the **New Password** parameter. If there is a failure the "Account Status" will indicate that the new password failed.

Account Status

This is a read-only field that provides information on the current activity for that screen. For instance, if adding a new user was successful a message will be displayed indicating the user has been added.

5.16 DELETE USER

An example of the CMM4 Delete User tab is displayed in Figure 28.

Figure 28: Delete User Tab of CMM4, Example

If you are of ADMINISTRATOR level and want to remove a user, the Delete Users Password tab allows you to do so as follows:

User

Use the down arrow to select the user you want to remove.

Delete

Ensure that the intended user is selected. Then click this button.

Account Status

This is a read-only field that provides information on the current activity for that screen. For instance, if deleting the user was successful a message will be displayed indicating the user has been deleted.

6 INSTALLING A CMM4

Ensure that you comply with standard local or national electrical and climbing procedures when you install the CMM4.

WARNING!

Installing a CMM involves electrical power and can involve height and exposure to RF (Radio Frequency) energy. To avoid personal injury, know and follow applicable national and local safety regulations and industry best practices, and follow the specific guidelines in this document

6.1 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.

6.2 GROUNDING EQUIPMENT

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

6.2.1 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 modules, perform the following steps:

- Engage a grounding professional if you have any questions on grounding.
- 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.
- Plan to use an appropriate surge suppressor on any Ethernet cable at the point where it enters any building or structure.

Install your modules at least 2 feet (0.6 meters) below the tallest point on the tower, pole, or roof.

6.3 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 U.S.A. If you are uncertain of code requirements, engage the services of a licensed electrician.

6.4 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 weather-resistant tape.

The cable can be a path for water to follow to enter the cable connector or even the module. You can prevent this problem by including and securing a drip loop where the cable enters the module enclosure.

6.5 TESTING THE COMPONENTS

The best practice is to connect all the components - BHs, APs, GPS antenna, and CMM4 - in a test setting and initially configure and verify them before deploying them to an installation. However, circumstances or local practice may require a different practice.

6.6 UNPACKING COMPONENTS

When you receive Canopy 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.

6.7 CABLES

Information on cable planning, ordering, and design is covered in Section 4.3 on page 23.

6.8 INSTALLING A GPS ANTENNA

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

Recommended Tools for GPS Antenna Mounting

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

3/8” nut driver

12” adjustable wrench

7/16” wrench

Needle-nose pliers

Mounting a GPS Antenna

Perform the following procedure to mount a GPS antenna.

Procedure 3: Mounting the GPS antenna

========== **Start of procedure** ==========

1. Ensure that the mounting position
   a. has an unobstructed view of the sky to 20º above the horizon.
   b. is not the highest object at the site. (The GPS antenna does not need to be particularly high on a site, which would give it more exposure to lightning. It just needs to have an unobstructed view of the sky.)

c. is not further than 100 feet (30.4 meters) of cable from the CMM.

2. Select a pole that has an outside diameter of 1.25 to 1.5 inches (3 to 4 cm) to which the GPS antenna bracket can be mounted.
3. Place the U-bolts (provided) around the pole as shown in Figure 29.
4. Slide the GPS antenna bracket onto the U-bolts.
5. Slide the ring washers (provided) onto the U-bolts.
6. Slide the lock washers (provided) onto the U-bolts.
7. Use the nuts (provided) to securely fasten the bracket to the U-bolts.

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

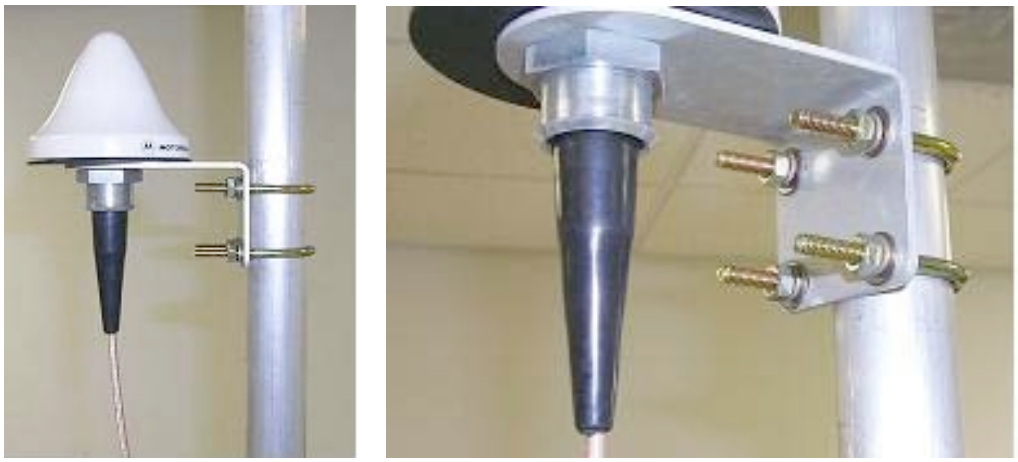


Figure 29: Detail of GPS antenna mounting

6.8.1 Cabling the GPS Antenna

Connect the GPS coax cable to the female N-connector on the GPS antenna. Information on the coax cable is covered in Section 4.3.2 on page 25.

6.9 INSTALLING THE POWER SUPPLY FOR THE CMM4

WARNING!

Although the output of the power supply is 29 V, the power rating classifies the converter as a Class 2 electric device. For this reason, whenever you work on power in the CMM4, you must *first* disconnect the DC supply from the AC power source.

Perform the following procedure to install the power supply.

Procedure 4: Installing the Power Supply for the CMM4

========== **Start of procedure** ==========

1. Install the CMM4 power supply in a hut, wiring closet, or weatherized NEMA-approved enclosure. It is designed for extreme temperatures but it is imperative to keep moisture away from the power converter.

2. Do not install the power supply within the CMM4 enclosure as it will increase the heat within the enclosure to an unacceptable level. The CMM4 enclosure is large to provide surface area for heat dissipation without the use of forced convection fans, not to provide space for additional high-power electronics.
3. Connect an AC/Mains power cord to the power supply (but not yet to an AC/Mains receptacle).
4. Choose and use a power cord as follows:
   d. If mounting the CMM4 either inside with the power supply or outside within 9 ft (2.8 m) of the power supply, use the 10-ft (3-m) of DC power cable (rated for outdoor use) attached to the power supply.
   e. If mounting the unit outside and further than 9 ft (2.8 m) from the power supply, engineer additional length of cable. Use either UV-resistant cable or shield the cable (as in a conduit) from UV rays.
5. Use a terminal block, connector, or splice inside a weatherized enclosure. to add the additional length.

   Table 6: Wire size for CMM4 power runs of longer than 9 feet (2.8 m)

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

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

6.10 TEMPERATURE RANGE

Install the CMM4 outside only when temperatures are above –4° F (–20° C). The gland openings and the bushings and inserts in the gland openings are rated for the full –40° to +131° F (–40° to +55° C) range of the CMM4. However, for dynamic operations (loosening, tightening, and inserting), they are compliant at, and rated for, only temperatures at or above –4° F (–20° C).

6.11 INSTALLING A CMM4

Prizm treats the EtherWAN Switch in a CMM4 as a generic switch. For Prizm to correctly associate each EtherWAN Switch with its CMM4

- before you install the CMM4, read and note the MAC address of both the CMM4 controller and EtherWAN switch from the physical units.
- after you discover a CMM4 and its switch, use these MAC addresses for moving the switch to the place in your Prizm network where the CMM4 was discovered.
- always maintain a record that associates these two MAC addresses.

IMPORTANT!

When Prizm discovers an EtherWAN switch in your network, it can't tell which CMM4 the switch is associated with, nor can it tell CMM4 EtherWAN switches from any other EtherWAN switches you may have in your network. The pair of MAC addresses you record directly from the CMM4 and its EtherWAN switch are the only means for you to establish the logical connection.

Perform the following procedure to install the CMM4.

Procedure 5: Mounting the CMM4

========== **Start of procedure** ==========

1. Ensure that the mounting position
   a. *is not* further than 328 feet (100 meters) from the furthest AP or BH that the CMM4 will serve.
   b. *is not* closer than 10 feet (3 meters) to the nearest AP or BH.
   c. *is not* further than 100 feet (30.5 meters) of cable from the intended mounting position of the GPS antenna.
   d. allows you to fully open the door for service.
2. Select a support structure to which the flanges can be mounted.
3. If the support structure is a wall, use screws or bolts (neither is provided) to attach the flanges to the wall.

   If the support structure is an irregular-shaped object, use adjustable stainless steel bands (provided) to attach the CMM4 to the object.

   If the support structure is a pole that has an outside diameter of 1.25 to 3 inches (3 to 8 cm), use a toothed V-bracket (provided) to
   a. attach the V-bracket to the pole as shown in Figure 30.

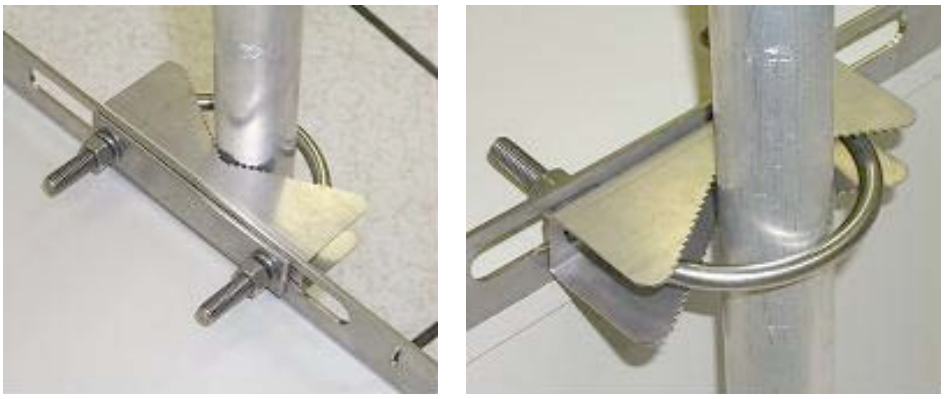


Figure 30: CMM4 V-bracket to pole mounting

   b. attach the CMM4 flanges to the V-bracket.

4. If the CMM4 is mounted to a non-conducting structure (cinder block wall, for example) or there is any doubt as to a good ground through the structure, run a 10 AWG ground cable from one of the Ground/Earth terminations of one of the terminal blocks inside the CMM4, through a cable gland, and to known good ground.

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

6.12 CABLING A CMM4

Perform the following procedure to cable the CMM4:

Procedure 6: Cabling the CMM4

========== **Start of procedure** ==========

1. Review the diagram inside the door of the CMM4.
2. Note that the inserts in the gland openings have precut holes.
3. Route Ethernet cables through the cable gland connectors to the Ethernet ports inside the CMM4 cabinet (see the grey cables in Figure 31). Stagger the cables (see Figure 32) to make it easier to feed them through the gland.

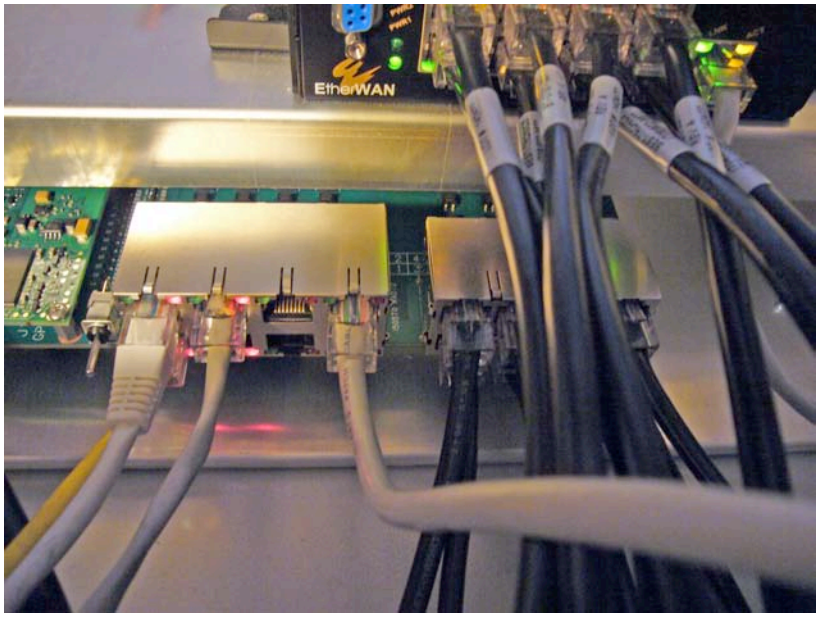


Figure 31: Ethernet Port Connections

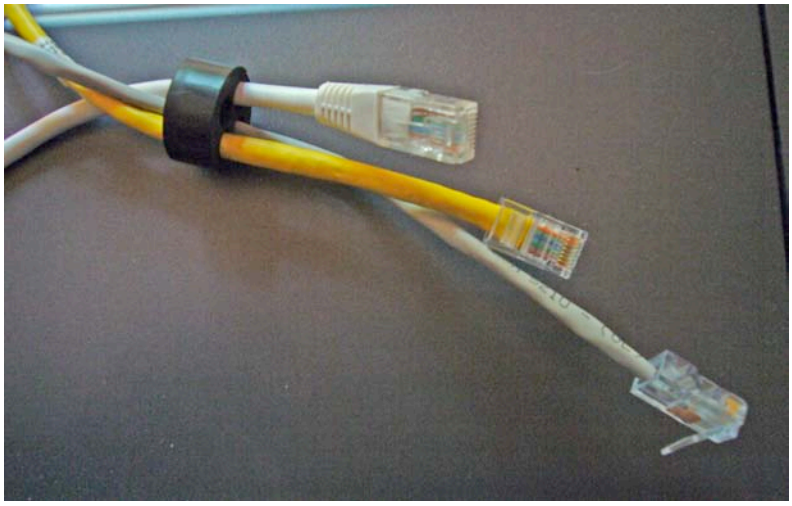


Figure 32: Staggered Ethernet Cables

4. Connect Ethernet cables as follows (see section 4.1 on page 19 for typical diagrams and planning information):
   a. **APs, BH10s, or BH20s (PTP 100 Series bridges):** cable to powered ports of the cluster controller. The cluster controller provides sync, power, and surge suppression for these connections. If the CMM4 is mounted inside a building or communications hut, a Motorola 600SSC surge suppressor should be mounted outside the building or communications hut on each line at the point of cable penetration to prevent over-voltages and over-currents from entering the building and potentially damaging other electronic equipment.
   b. **Terrestrial feeds under 100 Mbps (10/100BaseT):** cable to an unpowered port of the cluster controller. The cluster controller provides surge suppression for these connections. If the CMM4 is mounted inside a building or communications hut, a Motorola 600SSC surge suppressor should be mounted outside the building or communications hut on each line at the point of cable penetration to prevent over-voltages and over-currents from entering the building and potentially damaging other electronic equipment.
   c. **Terrestrial feeds over 100 Mbps (1000BaseT Gigabit Ethernet):** cable directly to the Gigabit port of the EtherWAN switch, and mount a Motorola PTP-LPU lightning protection unit or equivalent
      - within 3 ft (1 m) of the CMM4 if the CMM4 is located outdoors
      - on the outside of the building or communications hut at the point of cable penetration if the CMM4 is located indoors.
   d. **PTP 400 Series bridges:** cable to an unpowered port of the cluster controller. If the CMM4 is inside a building or communication hut, install the bridge's PIDU (Powered InDoor Unit) also inside the building, and and install a Motorola PTP-LPU lightning protection unit or equivalent on the outside of the building or communications hut at the point of cable penetration. If the CMM4 is mounted outside, locate the PIDU in a weather-tight enclosure within 3 ft (1 m) of the CMM4 and install a Motorola PTP-LPU lightning protection unit or equivalent within 3 ft (1 m) of the PIDU.

e. **PTP 500 and 600 Series bridges:** cable directly to the Gigabit port of the EtherWAN switch. If the CMM4 is inside a building or communication hut, install the bridge's PIDU (Powered InDoor Unit) also inside the building, and and install a Motorola PTP-LPU lightning protection unit or equivalent on the outside of the building or communications hut at the point of cable penetration. If the CMM4 is mounted outside, locate the PIDU in a weather-tight enclosure within 3 ft (1 m) of the CMM4 and install a Motorola PTP-LPU lightning protection unit or equivalent within 3 ft (1 m) of the PIDU.

5. On the door label, record the MAC and IP addresses of the CMM4 and all connected equipment.
6. Record also the MAC address of the EtherWAN switch.
7. Consistent with practices in your company, note the above information to add later to the company equipment database.
8. Connect the coax cable from the female N-connector on the GPS antenna to the female N-connector on the outside of the CMM4.
9. Ensure there is an Ethernet cable between the management port on the controller board and one of the Ethernet ports on the EtherWAN switch.
10. Feed the DC power cord through a cable gland. A 1-hole gland insert is provided, as the DC power cable is too thick to share a gland with other cables. The 1-hole insert is either connected to one of the patch cables or included in the parts bag.
11. Connect the white wire to +V on either of the 29 VDC terminal blocks.
12. Connect the black wire to −V (return and ground) on the same 29 VDC terminal block.
13. Plug the DC power supply into an AC receptacle (AC mains).
14. Verify that the LEDs light.

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

The indicator LEDs are shown in Figure 33. Color indicates position, but not state. For example, the red Power LED, in the left most position, lights when power is applied to the unit, but does not change color at any point.

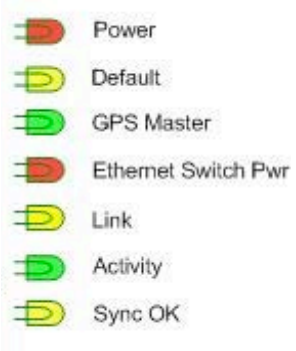


Figure 33: LED indicators

CAUTION!

Surge suppressors should be installed on any cables where they enter a building to reduce the possibility of overvoltages or overcurrents damaging any equipment in the building.

The following equipment, mounted outside of a communications hut or building at the point where the cables penetrate the building, is recommended:

- 600SSC for any data lines
- 200SS for DC cables
- A Polyphaser surge suppressor on the coax from the GPS antenna

6.13 POWER FAULTS

If excessive current is drawn on a port, the analog circuitry reports a PoE fault. The system then turns the port power off. The power will be restored when the fault is removed. Figure 34 shows the port status screen with a power fault on port 1.

Port Status

Port Number	1	2	3	4	5	6	7	8
Port Text	Port 1 Description	Port 2 Description	Port 3 Description	Port 4 Description	Port 5 Description	Port 6 Description	Port 7 Description	Port 8 Description
Power	Power Fault! 0 V	29 V	29 V	29 V	29 V	29 V	29 V	29 V
Device Type	Canopy	Canopy	Canopy	Canopy	Canopy	Canopy	Canopy	Canopy

Power fault on port:1
Please check the devices and port configurations.

Figure 34: Port Status Showing Power Fault

7 REGULATORY AND LEGAL NOTICES

7.1 IMPORTANT NOTE ON MODIFICATIONS

Intentional or unintentional changes or modifications to the equipment must not be made unless under the express consent of the party responsible for compliance. Any such modifications could void the user's authority to operate the equipment and will void the manufacturer's warranty.

7.2 NATIONAL AND REGIONAL REGULATORY NOTICES

7.2.1 U.S. Federal Communication Commission (FCC) Notification

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the US FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with these instructions, may cause harmful interference to radio communications. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment on and off, the user is encouraged to correct the interference by one or more of the following measures:

- Increase the separation between the affected equipment and the unit;
- Connect the affected equipment to a power outlet on a different circuit from that which the receiver is connected to;
- Consult the dealer and/or experienced radio/TV technician for help.

7.2.2 Industry Canada (IC) Notification

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to RSS-210 of Industry Canada. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with these instructions, may cause harmful interference to radio communications. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment on and off, the user is encouraged to correct the interference by one or more of the following measures:

- Increase the separation between the affected equipment and the unit;
- Connect the affected equipment to a power outlet on a different circuit from that which the receiver is connected to;
- Consult the dealer and/or experienced radio/TV technician for help.

To reduce potential radio interference to other users, the antenna type and its gain should be chosen so its Equivalent Isotropic Radiated Power (EIRP) is not more than that permitted for successful communication.

7.2.3 Equipment Disposal

Waste (Disposal) of Electronic and Electric Equipment

Please do not dispose of Electronic and Electric Equipment or Electronic and Electric Accessories with your household waste. In some countries or regions, collection systems have been set up to handle waste of electrical and electronic equipment. In European Union countries, please contact your local equipment supplier representative or service center for information about the waste collection system in your country.

7.2.4 EU Declaration of Conformity for RoHS Compliance

Motorola hereby, declares that these Motorola products are in compliance with the essential requirements and other relevant provisions of Directive 2002/95/EC, Restriction of the use of certain Hazardous Substances (RoHS) in electrical and electronic equipment.

The relevant Declaration of Conformity can be found at http://www.canopywireless.com/doc.php.

7.2.5 Labeling and Disclosure Table for China

The People's Republic of China requires that Motorola's products comply with China Management Methods (CMM) environmental regulations. (China Management Methods refers to the regulation *Management Methods for Controlling Pollution by Electronic Information Products*.) Two items are used to demonstrate compliance; the label and the disclosure table.

The label is placed in a customer visible position on the product.

- Logo 1 means that the product contains no substances in excess of the maximum concentration value for materials identified in the China Management Methods regulation.
- Logo 2 means that the product may contain substances in excess of the maximum concentration value for materials identified in the China Management Methods regulation, and has an Environmental Friendly Use Period (EFUP) in years, fifty years in the example shown.

Logo 1  Logo 2 

The Environmental Friendly Use Period (EFUP) is the period (in years) during which the Toxic and Hazardous Substances (T&HS) contained in the Electronic Information Product (EIP) will not leak or mutate causing environmental pollution or bodily injury from the use of the EIP. The EFUP indicated by the Logo 2 label applies to a product and all its parts. Certain field-replaceable parts, such as battery modules, can have a different EFUP and are marked separately.

The Disclosure Table is intended only to communicate compliance with China requirements; it is not intended to communicate compliance with EU RoHS or any other environmental requirements.

部件名称	有毒有害物质或元素					
	铅 (Pb)	汞 (Hg)	镉 (Cd)	六价铬 (Cr^{6+})	多溴联苯 (PBB)	多溴二苯醚 (PBDE)
金属部件	×	○	×	×	○	○
电路模块	×	○	×	×	○	○
电缆及电缆组件	×	○	×	×	○	○
塑料和聚合物部件	○	○	○	○	○	×

表示该有毒有害物质在该部件所有均质材料中的含量均在SJ/T11363-2006 标准规定的限量要求以下。

表示该有毒有害物质至少在该部件的某一均质材料中的含量超出SJ/T11363-2006 标准规定的限量要求。

Table 7: China Management Methods Disclosure Table

7.3 RF EXPOSURE SEPARATION DISTANCES FOR CANOPY RADIOS

To protect from overexposure to radio frequency (RF) energy, install Canopy radios so as to provide and maintain the minimum separation distances from all persons shown in Table 8.

Table 8: Exposure separation distances

Module Type	Separation Distance from Persons
Canopy Module	At least 20 cm (approx 8 in)
Canopy Module with Reflector Dish	At least 1.5 m (approx 60 in or 5 ft)
Canopy 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)

For details and discussion of the associated calculations, see the Canopy System Release 8 User's Guide, available at http://motorola.canopywireless.com/support/library/

7.4 LEGAL NOTICES

7.4.1 Software License Terms and Conditions

ONLY OPEN THE PACKAGE, OR USE THE SOFTWARE AND RELATED PRODUCT IF YOU ACCEPT THE TERMS OF THIS LICENSE. BY BREAKING THE SEAL ON THIS DISK KIT / CDROM, OR IF YOU USE THE SOFTWARE OR RELATED PRODUCT, YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS, DO

NOT USE THE SOFTWARE OR RELATED PRODUCT; INSTEAD, RETURN THE SOFTWARE TO PLACE OF PURCHASE FOR A FULL REFUND. THE FOLLOWING AGREEMENT IS A LEGAL AGREEMENT BETWEEN YOU (EITHER AN INDIVIDUAL OR ENTITY), AND MOTOROLA, INC. (FOR ITSELF AND ITS LICENSORS). THE RIGHT TO USE THIS PRODUCT IS LICENSED ONLY ON THE CONDITION THAT YOU AGREE TO THE FOLLOWING TERMS.

Now, therefore, in consideration of the promises and mutual obligations contained herein, and for other good and valuable consideration, the receipt and sufficiency of which are hereby mutually acknowledged, you and Motorola agree as follows:

Grant of License. Subject to the following terms and conditions, Motorola, Inc., grants to you a personal, revocable, non-assignable, non-transferable, non-exclusive and limited license to use on a single piece of equipment only one copy of the software contained on this disk (which may have been pre-loaded on the equipment)(Software). You may make two copies of the Software, but only for backup, archival, or disaster recovery purposes. On any copy you make of the Software, you must reproduce and include the copyright and other proprietary rights notice contained on the copy we have furnished you of the Software.

Ownership. Motorola (or its supplier) retains all title, ownership and intellectual property rights to the Software and any copies,

including translations, compilations, derivative works (including images) partial copies and portions of updated works. The Software is Motorola's (or its supplier's) confidential proprietary information. This Software License Agreement does not convey to you any interest in or to the Software, but only a limited right of use. You agree not to disclose it or make it available to anyone without Motorola's written authorization. You will exercise no less than reasonable care to protect the Software from unauthorized disclosure. You agree not to disassemble, decompile or reverse engineer, or create derivative works of the Software, except and only to the extent that such activity is expressly permitted by applicable law.

Termination. This License is effective until terminated. This License will terminate immediately without notice from Motorola or judicial resolution if you fail to comply with any provision of this License. Upon such termination you must destroy the Software, all accompanying written materials and all copies thereof, and the sections entitled Limited Warranty, Limitation of Remedies and Damages, and General will survive any termination.

Limited Warranty. Motorola warrants for a period of ninety (90) days from Motorola's or its customer's shipment of the Software to you that (i) the disk(s) on which the Software is recorded will be free from defects in materials and workmanship under normal use and (ii) the Software, under normal use, will perform substantially in accordance with Motorola's published specifications for that release level of the Software. The written materials are provided "AS IS" and without warranty of any kind. Motorola's entire liability and your sole and exclusive remedy for any breach of the foregoing limited warranty will be, at Motorola's option, replacement of the disk(s), provision of downloadable patch or replacement code, or refund of the unused portion of your bargained for contractual benefit up to the amount paid for this Software License.

THIS LIMITED WARRANTY IS THE ONLY WARRANTY PROVIDED BY MOTOROLA, AND MOTOROLA AND ITS LICENSORS EXPRESSLY DISCLAIM ALL OTHER WARRANTIES, EITHER EXPRESS OF IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. MOTOROLA DOES NOT WARRANT THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT DEFECTS IN THE SOFTWARE WILL BE CORRECTED. NO ORAL OR WRITTEN REPRESENTATIONS MADE BY MOTOROLA OR AN AGENT THEREOF SHALL CREATE A WARRANTY OR IN ANY WAY INCREASE THE SCOPE OF THIS WARRANTY. MOTOROLA DOES NOT WARRANT ANY SOFTWARE THAT HAS BEEN OPERATED IN EXCESS OF SPECIFICATIONS, DAMAGED, MISUSED, NEGLECTED, OR IMPROPERLY INSTALLED. BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF IMPLIED WARRANTIES, THE ABOVE LIMITATIONS MAY NOT APPLY TO YOU.

Limitation of Remedies and Damages. Regardless of whether any remedy set forth herein fails of its essential purpose, IN NO EVENT SHALL MOTOROLA OR ANY OF THE LICENSORS, DIRECTORS, OFFICERS, EMPLOYEES OR AFFILIATES OF THE FOREGOING BE LIABLE TO YOU FOR ANY CONSEQUENTIAL, INCIDENTAL, INDIRECT, SPECIAL OR SIMILAR DAMAGES WHATSOEVER (including, without limitation, damages for loss of business profits, business interruption, loss of business information and the like), whether foreseeable or unforeseeable, arising out of the use or inability to use the Software or accompanying written materials, regardless of the basis of the claim and even if Motorola or a Motorola representative has been advised of the possibility of such damage. Motorola's liability to you for direct damages for any cause whatsoever, regardless of the basis of the form of the action, will be limited to the price paid for the Software that caused the damages. THIS LIMITATION WILL NOT APPLY IN CASE OF PERSONAL INJURY ONLY WHERE AND TO THE EXTENT THAT APPLICABLE LAW REQUIRES SUCH LIABILITY. BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

Maintenance and Support. Motorola shall not be responsible for maintenance or support of the software. By accepting the license granted under this agreement, you agree that Motorola will be under no obligation to provide any support, maintenance or service in connection with the Software or any application developed by you. Any maintenance and support of the Related Product will be provided under the terms of the agreement for the Related Product.

Transfer. In the case of software designed to operate on Motorola equipment, you may not transfer the Software to another party except: (1) if you are an end-user, when you are transferring the Software together with the Motorola equipment on which it operates; or 2) if you are a Motorola licensed distributor, when you are transferring the Software either together with such Motorola equipment or are transferring the Software as a licensed duly paid for upgrade, update, patch, new release, enhancement or replacement of a prior version of the Software. If you are a Motorola licensed distributor, when you are transferring the Software as permitted herein, you agree to transfer the Software with a license agreement having terms and conditions no less restrictive than those contained herein. You may transfer all other Software, not otherwise having an agreed restriction on transfer, to another party. However, all such transfers of Software are strictly subject to the conditions precedent that the other party agrees to accept the terms and conditions of this License, and you destroy any copy of the Software you do not transfer to that party. You may not sublicense or otherwise transfer, rent or lease the Software without our written consent. You may not transfer the Software in violation of any laws, regulations, export controls or economic sanctions imposed by the US Government.

Right to Audit. Motorola shall have the right to audit annually, upon reasonable advance notice and during normal business hours, your records and accounts to determine compliance with the terms of this Agreement.

Export Controls. You specifically acknowledge that the software may be subject to United States and other country export control laws. You shall comply strictly with all requirements of all applicable export control laws and regulations with respect to all such software and materials.

US Government Users. If you are a US Government user, then the Software is provided with "RESTRICTED RIGHTS" as set forth in subparagraphs (c)(1) and (2) of the Commercial Computer Software-Restricted Rights clause at FAR 52 227-19 or subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013, as applicable.

Disputes. You and Motorola hereby agree that any dispute, controversy or claim, except for any dispute, controversy or claim involving intellectual property, prior to initiation of any formal legal process, will be submitted for non-binding mediation, prior to initiation of any formal legal process. Cost of mediation will be shared equally. Nothing in this Section will prevent either party from resorting to judicial proceedings, if (i) good faith efforts to resolve the dispute under these procedures have been unsuccessful, (ii) the dispute, claim or controversy involves intellectual property, or (iii) interim relief from a court is necessary to prevent serious and irreparable injury to that party or to others.

General. Illinois law governs this license. The terms of this license are supplemental to any written agreement executed by both parties regarding this subject and the Software Motorola is to license you under it, and supersedes all previous oral or written communications between us regarding the subject except for such executed agreement. It may not be modified or waived except in writing and signed by an officer or other authorized representative of each party. If any provision is held invalid, all other provisions shall remain valid, unless such invalidity would frustrate the purpose of our agreement. The failure of either party to enforce any rights granted hereunder or to take action against the other party in the event of any breach hereunder shall not be deemed a waiver by that party as to subsequent enforcement of rights or subsequent action in the event of future breaches.

7.4.2 Hardware Warranty in U.S.

Motorola U.S. offers a warranty covering a period of one year from the date of purchase by the customer. If a product is found defective during the warranty period, Motorola will repair or replace the product with the same or a similar model, which may be a reconditioned unit, without charge for parts or labor.

7.4.3 Limit of Liability

IN NO EVENT SHALL MOTOROLA BE LIABLE TO YOU OR ANY OTHER PARTY FOR ANY DIRECT, INDIRECT, GENERAL, SPECIAL, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY OR OTHER DAMAGE ARISING OUT OF THE USE OR INABILITY TO USE THE PRODUCT (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION OR ANY OTHER PECUNIARY LOSS, OR FROM ANY BREACH OF WARRANTY, EVEN IF MOTOROLA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. (Some states do not allow the exclusion or limitation of incidental or consequential damages, so the above exclusion or limitation may not apply to you.) IN NO CASE SHALL MOTOROLA'S LIABILITY EXCEED THE AMOUNT YOU PAID FOR THE PRODUCT.

8 ADDITIONAL RESOURCES

A community forum and a knowledge base are available where you can find answers and raise questions.

Canopy Community Forums at http://motorola.canopywireless.com/support/community/.
This resource facilitates communication with other users and with authorized Canopy experts. Available forums include General Discussion, Network Monitoring Tools, and Suggestions.

Canopy Knowledge Base at http://motorola.canopywireless.com/support/knowledge.
This resource facilitates exploration and searches, provides recommendations, and describes tools. Available categories include

General (Answers to general questions provide an overview of the Canopy system.)

Product Alerts

Helpful Hints

FAQs (frequently asked questions)

Hardware Support

Software Support

Tools

Glossary

9 GLOSSARY

10Base-T	Technology in Ethernet communications that can deliver 10 Mb of data across 328 feet (100 meters) of CAT 5 cable.
100Base-TX	Technology in Ethernet communications that can deliver 100 Mb of data across 328 feet (100 meters) of CAT 5 cable.
169.254.0.0	Gateway IP address default in modules.
169.254.1.1	IP address default in modules.
169.254.x.x	IP address default in Microsoft and Apple operating systems without a DHCP (Dynamic Host Configuration Protocol) server.
255.255.0.0	Subnet mask default in modules and in Microsoft and Apple operating systems.
802.3	An IEEE standard that defines the contents of frames that are transferred through Ethernet connections. Each of these frames contains a preamble, the address to which the frame is sent, the address that sends the frame, the length of the data to expect, the data, and a checksum to validate that no contents were lost.
802.11	The IEEE standard for wireless local area networks.
802.15	The IEEE standard for wireless personal area networks.
Access Point Cluster	Two to six Access Point Modules that together distribute network or Internet services to a community of 1,200 or fewer subscribers. Each Access Point Module covers a 60° sector. This cluster covers as much as 360°. Also known as AP cluster.
Access Point Module	Also known as AP. One module that distributes network or Internet services in a 60° sector to 200 subscribers or fewer.
Address Resolution Protocol	Protocol defined in RFC 826 to allow a network element to correlate a host IP address to the Ethernet address of the host. See http://www.faqs.org/rfcs/rfc826.html.
AP	Access Point Module. One module that distributes network or Internet services in a 60° sector to 200 subscribers or fewer.
APA	Access Point module address.

ARP	Address Resolution Protocol. A protocol defined in RFC 826 to allow a network element to correlate a host IP address to the Ethernet address of the host. See http://www.faqs.org/rfcs/rfc826.html.
Backhaul Module	Also known as BH. A module that provides point-to-point connectivity as either a standalone link or a link to an Access Point cluster through a selected Access Point Module. See also Backhaul Timing Master and Backhaul Timing Slave.
Backhaul Timing Master	Backhaul Module that sends network timing (synchronization) to another Backhaul Module, which serves as the Backhaul timing slave.
Backhaul Timing Slave	Backhaul Module that receives network timing (synchronization) from another Backhaul Module, which serves as the Backhaul timing master.
BH	Backhaul Module. A module that provides point-to-point connectivity as either a standalone link or a link to an Access Point cluster through a selected Access Point Module.
Canopy	Motorola's Point-to-Multipoint system operating designed to operate in the interference environment typical of unlicensed spectrum
CAT 5 Cable	Cable that delivers Ethernet communications from module to module. Modules auto-sense whether this cable is wired in a straight-through or crossover scheme.
Cluster Management Module	Module that provides power, GPS timing, and networking connections for an AP cluster. Also known as CMM.
CMM	Cluster Management Module. A module that provides power, GPS timing, and networking connections for an Access Point cluster. If this CMM4is connected to a Backhaul Module (BH), then this CMM4is the central point of connectivity for the entire site.
Community String Field	Control string that allows an element management system or other SNMP-based system access to the SNMP MIB in a module.
DHCP	Dynamic Host Configuration Protocol, defined in RFC 2131. Protocol that 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 a system. See http://www.faqs.org/rfcs/rfc2131.html. See also Static IP Address Assignment.

DiffServ	Differentiated Services, consistent with RFC 2474. A byte in the type of service (TOS) field of packets whose values correlates to the channel on which the packet should be sent. The value is a numeric code point. The system maps each of 64 code points to values of 0 through 7. Three of these code points have fixed values, and the remaining 61 are settable. Values 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. Among the settable parameters, the values are set in the AP for all downlinks within the sector and in the SM for each uplink.
Disable	To turn off a feature in the module after both the feature activation file has *activated* the module to use the feature and the operator has *enabled* the feature in the module. See also Activate and Enable.
Dynamic Host Configuration Protocol	Protocol defined in RFC 2131 that enables a device to be assigned a new IP address and TCP/IP parameters, including a default gateway, whenever the device reboots. Thus Dynamic Host Configuration Protocol reduces configuration time, conserves IP addresses, and allows modules to be moved to a different network within the system. See http://www.faqs.org/rfcs/rfc2131.html. See also Static IP Address Assignment.
Electronic Serial Number	Hardware address that the factory assigns to the module for identification in the Data Link layer interface of the Open Systems Interconnection system. This address serves as an electronic serial number. Same as MAC Address.
Enable	To turn on a feature in the module after the feature activation file has *activated* the module to use the feature. See also Activate.
ESN	Electronic Serial Number. The hardware address that the factory assigns to the module for identification in the Data Link layer interface of the Open Systems Interconnection system. This address serves as an electronic serial number. Same as MAC Address.
EthBusErr Field	This field displays how many Ethernet bus errors occurred on the Ethernet controller.
Ethernet Protocol	Any of several IEEE standards that define the contents of frames that are transferred from one network element to another through Ethernet connections.
FCC	Federal Communications Commission of the U.S.A.
Feature Activation Key	Software key file whose file name includes the ESN of the target module. When installed on the module, this file *activates* the module to have the feature *enabled* or disabled in a separate operator action.
Field-programmable Gate Array	Array of logic, relational data, and wiring data that is factory programmed and can be reprogrammed.

File Transfer Protocol	Utility that transfers of files through TCP (Transport Control Protocol) between computing devices that do not operate on the same platform. Defined in RFC 959. See http://www.faqs.org/rfcs/rfc959.html.
FPGA	Field-programmable Gate Array. An array of logic, relational data, and wiring data that is factory programmed and can be reprogrammed.
FTP	File Transfer Protocol, defined in RFC 959. Utility that transfers of files through TCP (Transport Control Protocol) between computing devices that do not operate on the same platform. See http://www.faqs.org/rfcs/rfc959.html.
Global Positioning System	Network of satellites that provides absolute time to networks on earth, which use the time signal to synchronize transmission and reception cycles (to avoid interference) and to provide reference for troubleshooting activities.
GPS	Global Positioning System. A network of satellites that provides absolute time to networks on earth, which use the time signal to synchronize transmission and reception cycles (to avoid interference) and to provide reference for troubleshooting activities.
GPS/3	Third-from-left LED in the module. In the operating mode for an Access Point Module or Backhaul timing master, this LED is continuously lit as the module receives sync pulse. In the operating mode for a Subscriber Module or a Backhaul timing slave, this LED flashes on and off to indicate that the module is not registered. In the aiming mode for a Subscriber Module or a Backhaul timing slave, this LED is part of a bar graph that indicates the quality of the RF link.
GUI	Graphical user interface.
High-priority Channel	Channel that supports low-latency traffic (such as Voice over IP) over low-latency traffic (such as standard web traffic and file downloads). To recognize the latency tolerance of traffic, this channel reads the IPv4 Type of Service Low Latency bit.
HTTP	Hypertext Transfer Protocol, used to make the Internet resources available on the World Wide Web. Defined in RFC 2068. See http://www.faqs.org/rfcs/rfc2068.html.
ICMP	Internet Control Message Protocols defined in RFC 792, used to identify Internet Protocol (IP)-level problems and to allow IP links to be tested. See http://www.faqs.org/rfcs/rfc792.html.
inucastpkts count Field	How many inbound subnetwork-unicast packets were delivered to a higher-layer protocol.
inunknownprotos count Field	How many inbound packets were discarded because of an unknown or unsupported protocol.

IP	Internet Protocol defined in RFC 791. The Network Layer in the TCP/IP protocol stack. This protocol is applied to addressing, routing, and delivering, and re-assembling data packets into the Data Link layer of the protocol stack. See http://www.faqs.org/rfcs/rfc791.html.
IP Address	32-bit binary number that identifies a network element by both network and host. See also Subnet Mask.
IPv4	Traditional version of Internet Protocol, which defines 32-bit fields for data transmission.
ISM	Industrial, Scientific, and Medical Equipment radio frequency band, in the 900-MHz, 2.4-GHz, and 5.8-GHz ranges.
LOS	Line of sight. The wireless path (not simply visual path) direct from module to module. The path that results provides both ideal aim and an ideal Fresnel zone.
LUID	Logical Unit ID. The final octet of the 4-octet IP address of the module.
MAC Address	Media Access Control address. The hardware address that the factory assigns to the module for identification in the Data Link layer interface of the Open Systems Interconnection system. This address serves as an electronic serial number.
Master	Designation that defines the role of a component relative to the role of another. This designation both applies to a Backhaul module that provides synchronization over the air to another Backhaul module (a Backhaul timing slave) and applies to a Bandwidth and Authentication Manager (BAM) server whose SQL database is automatically copied onto a redundant BAM server (BAM slave). In each case, the master is not a product. Rather, the master is the role that results from deliberate configuration steps.
Media Access Control Address	Hardware address that the factory assigns to the module for identification in the Data Link layer interface of the Open Systems Interconnection system. This address serves as an electronic serial number.
MIB	Management Information Base. Space that allows a program (agent) in the network to relay information to a network monitor about the status of defined variables (objects).
NAT	Network Address Translation defined in RFC 1631. A scheme that isolates Subscriber Modules from the Internet. See http://www.faqs.org/rfcs/rfc1631.html.
NBI	See Northbound Interface.
NEC	National Electrical Code. The set of national wiring standards that are enforced in the U.S.A.

NetBIOS	Protocol defined in RFC 1001 and RFC 1002 to support an applications programming interface in TCP/IP. This interface allows a computer to transmit and receive data with another host computer on the network. RFC 1001 defines the concepts and methods. RFC 1002 defines the detailed specifications. See http://www.faqs.org/rfcs/rfc1001.html and http://www.faqs.org/rfcs/rfc1002.html.
Network Address Translation	Scheme that defines the Access Point Module as a proxy server to isolate registered Subscriber Modules from the Internet. Defined in RFC 1631. See http://www.faqs.org/rfcs/rfc1631.html.
Network Management Station	Monitor device that uses Simple Network Management Protocol (SNMP) to control, gather, and report information about predefined network variables (objects).
NMS	Network Management Station. A monitor device that uses Simple Network Management Protocol (SNMP) to control, gather, and report information about predefined network variables (objects).
Northbound Interface	The interface within Prizm to higher-level systems. This interface consists of a Simple Network Management Protocol (SNMP) agent for integration with a network management system (NMS); a Simple Object Access Protocol (SOAP) XML-based application programming interface (API) for web services that supports integration with an operations support systems (OSS) such as a customer relationship management (CRM), billing, or provisioning system; and console automation that allows such higher-level systems to launch and appropriately display the PrizmEMS management console in a custom-developed GUI.
Point-to-Point Protocol	Standards that RFC 1661 defines for data transmittal on the Internet. Also known as PPP or PTP. See http://www.faqs.org/rfcs/rfc1661.html.
Prizm	The software product that allows users to partition their entire networks into criteria-based subsets and independently monitor and manage those subsets. Prizm Release 1.0 and later includes a Northbound Interface to higher-level systems. Prizm Release 2.0 and later integrates Bandwidth and Authentication Manager (BAM) functionality and supports simple migration of a pre-existing authentication, bandwidth, and VLAN settings into the Prizm database.
Protective Earth	Connection to earth (which has a charge of 0 volts). Also known as ground.
Proxy Server	Network computer that isolates another from the Internet. The proxy server communicates for the other computer, and sends replies to only the appropriate computer, which has an IP address that is not unique or not registered.

PTMP	Point-to-Multipoint Protocol defined in RFC 2178, which specifies that data that originates from a central network element can be received by all other network elements, but data that originates from a non-central network element can be received by only the central network element. See http://www.faqs.org/rfcs/rfc2178.html.
PTP	Point-to-Point Protocol. The standards that RFC 1661 defines for data transmittal on the Internet. See http://www.faqs.org/rfcs/rfc1661.html.
QoS	Quality of Service. A frame field that Bandwidth and Authentication Manager (BAM) provides to the AP and SM the sustained data rates and burst data limits of the SM. The format of this field is 64 hexadecimal characters of 0 to 9 and a to f. The BAM SQL database expresses this field as five contiguous subfields.
Quality of Service	A frame bit that Bandwidth and Authentication Manager (BAM) provides to the AP and SM the sustained data rates and burst data limits of the SM. The format of this field is 64 hexadecimal characters of 0 to 9 and a to f. The BAM SQL database expresses this field as five contiguous subfields. Also known as QoS.
RF	Radio frequency. How many times each second a cycle in the antenna occurs, from positive to negative and back to positive amplitude.
RJ-11	Standard cable that is typically used for telephone line or modem connection.
RJ-45	Standard cable that is typically used for Ethernet connection. This cable may be wired as straight-through or as crossover. Later modules auto-sense whether the cable is straight-through or crossover.
Router	Network element that uses the logical (IP) address of another to pass data to only the intended recipient. Compare to Switch and Bridge.
Slave	Designation that defines the role of a component relative to the role of another. This designation both applies to a Backhaul slave that receives synchronization over the air from another Backhaul module (a Backhaul timing master) and applies to a redundant Bandwidth and Authentication Manager (BAM) server whose SQL database is automatically overwritten by a copy from the primary BAM server (BAM master). In each case, the slave is not a product. Rather, the slave is the role that results from deliberate configuration steps.
SM	Customer premises equipment (CPE) device that extends network or Internet services by communication with an Access Point Module or an Access Point cluster.

SNMP	Simple Network Management Protocol, defined in RFC 1157. A standard that is used for communications between a program (agent) in the network and a network management station (monitor). See http://www.faqs.org/rfcs/rfc1157.html.
SNMP Trap	Capture of information that informs the network monitor through Simple Network Management Protocol of a monitored occurrence in the module.
Subnet Mask	32-bit binary number that filters an IP address to reveal what part identifies the network and what part identifies the host. The number of subnet mask bits that are set to 1 indicates how many leading bits of the IP address identify the network. The number of subnet mask bits that are set 0 indicate how many trailing bits of the IP address identify the host.
Subscriber Module	Customer premises equipment (CPE) device that extends network or Internet services by communication with an Access Point Module or an Access Point cluster.
Switch	Network element that uses the port that is associated with the physical address of another to pass data to only the intended recipient. Compare to Bridge and Router.
Sync	GPS (Global Positioning System) absolute time, which is passed from one module to another. Sync enables timing that prevents modules from transmitting or receiving interference. Sync also provides correlative time stamps for troubleshooting efforts.
TCP	Alternatively known as Transmission Control Protocol or Transport Control Protocol. The Transport Layer in the TCP/IP protocol stack. This protocol is applied to assure that data packets arrive at the target network element and to control the flow of data through the Internet. Defined in RFC 793. See http://www.faqs.org/rfcs/rfc793.html.
tcp	Transport Control type of port. The Canopy system uses Port 3306:tcp for MySQL® database communications, Port 9080:tcp for SSE `telnet` communications, and Port 9090:tcp for Engine `telnet` communications.
telnet	Utility that allows a client computer to update a server. A firewall can prevent the use of the `telnet` utility to breach the security of the server. See http://www.faqs.org/rfcs/rfc818.html, http://www.faqs.org/rfcs/rfc854.html and http://www.faqs.org/rfcs/rfc855.html.
Textual Conventions MIB	Management Information Base file that defines Canopy system-specific textual conventions. See also Management Information Base.
TxUnderrun Field	This field displays how many transmission-underrun errors occurred on the Ethernet controller.

VID	VLAN identifier. See VLAN.
VLAN	Virtual local area network. An association of devices through software that contains broadcast traffic, as routers would, but in the switch-level protocol.
VPN	Virtual private network for communication over a public network. One typical use is to connect remote employees, who are at home or in a different city, to their corporate network over the Internet. Any of several VPN implementation schemes is possible. With the Network Address Translation feature (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.