28 MAINTAINING YOUR CYCLONE SOFTWARE

Cyclone provides release compatibility information and caveats about each release.

28.1 HISTORY OF SYSTEM SOFTWARE UPGRADES

28.1.1 Cyclone Release 8 Features

Cyclone Release 8 introduces the following new features:

- Scheduling Limited to Hardware Scheduler
- Tiered Permissions and User Accounts
- GUI Customizable via CSS
- Links to SM GUI via Session Status and Remote Subscribers Tabs of AP
- Dynamic Frequency Selection (DFS) v1.2.3 in All 5.4- and 5.7-GHz Modules
- Bit Error Rate (BER) Display with Hardware Scheduler
- AP SNMP Proxy to SMs
- Translation Bridging (MAC Address Mapping)
- SM Isolation
- Management Access Filtering for SM
- Source IP Management Access for AP and SM
- Optional DHCP Configuration of Management Interface

28.1.2 Cyclone Release 8 Fixes

Cyclone Release 8 includes the following fixes:

- Management Web (http) Access Lockup Fix
- Enforcement of Ethernet Link Speed Setting
- MIBs Support Only Applicable Objects

28.2 HISTORY OF CMMmicro SOFTWARE UPGRADES

- Cyclone currently supports CMMmicro Releases up through Release 2.2.

28.3 TYPICAL CONTENTS OF RELEASE NOTES

Cyclone supports each release with software release notes, which include

- description of features that are introduced in the new release.
- issues that the new release resolves.
- known issues and special notes for the new release.
- installation procedures for the new release.

28.4 TYPICAL UPGRADE PROCESS

In a typical upgrade process, proceed as follows:

1. Visit the software page of the Cyclone web site.
2. Read the compatibility information and any caveats that Cyclone associates with the release.
3. Read the software release notes from the web site.
4. On the basis of these, decide whether the release is appropriate for your network.
5. Download the software release and associated files.
6. Use CNUT to manage the upgrade across your network.

28.4.1 Downloading Software and Release Notes

All supported software releases, the associated software release notes document, and updated MIB files are available for download at any time from http://Last Mile Gear.Last Mile Gear.com/Cyclone/support/software/. This web site also typically provides a summary of the backward compatibility and any advantages or disadvantages of implementing the release.

When you click on the release that you wish to download, you are prompted for information that identifies yourself and your organization (such as name, address, and e-mail address). When you complete and submit the form that prompts for this information, the download is made available to you.

29 REBRANDING MODULE INTERFACE SCREENS

Distinctive fonts indicate

literal user input.
variable user input.
literal system responses.
variable system responses.

The interface screens on each module display the Cyclone or Cyclone Advantage logo. These logos can be replaced with other logos using Procedure 42.

The logo is a hyperlink and clicking on it takes the user to the Cyclone web site. A different site (perhaps the operator's support site) can be made the destination using Procedure 43.

To return a module to regular logos and hyperlinks, use Procedure 44.

The logo at the top of each page is a key indicator to the user whether a module is Cyclone or Cyclone Advantage. If you choose to replace the Cyclone logos, use two noticeably different logos so that users can continue to easily distinguish between a Cyclone module and a Cyclone Advantage module.

To replace logos and hyperlinks efficiently throughout your network, read the following two procedures, write a script, and execute your script through the Cyclone Network Updater Tool (CNUT).[7] To replace them individually, use one of the following two procedures.

Procedure 42: Replacing the Cyclone logo on the GUI with another logo

1. If the current logo is the Cyclone logo, name your custom logo file on your computer `Cyclone.jpg` and put it in your home directory.

   If the current logo is the Cyclone Advantage logo, name your custom logo file on your computer `advantaged.jpg` and put it in your home directory.

2. Use an FTP (File Transfer Protocol) session to transfer this file to the module, as in the example session shown in Figure 165.

[7] See Using the Cyclone Network Updater Tool (CNUT) on Page 181.

```
> ftp ModuleIPAddress
Connected to ModuleIPAddress
220 FTP server ready
Name (ModuleIPAddress:none): root
331 Guest login ok
Password: <password-if-configured>
230 Guest login ok, access restrictions apply.

ftp> binary
200 Type set to I
ftp> put Cyclone.jpg
     OR
     put advantaged.jpg
     OR
     put top.html
ftp> quit
221 Goodbye
```

Figure 165: Example ftp session to transfer custom logo file

3. Use a telnet session and the **addwebfile** command to add the new file to the file system, as in the example session shown in Figure 166.

NOTE:
Supported telnet commands execute the following results:

- **addwebfile** adds a custom logo file to the file system.
- **clearwebfile** clears the logo file from the file system.
- **lsweb** lists the custom logo file and display the storage space available on the file system.

```
>telnet ModuleIPAddress
/---------\
C A N O P Y

Last Mile Gear Broadband Wireless Technology
Center
(Copyright 2001, 2002 Last Mile Gear Inc.)

Login: root
Password: <password-if-configured>

Telnet +> addwebfile Cyclone.jpg
          OR
          addwebfile advantaged.jpg
          OR
          addwebfile top.html

Telnet +> lsweb

Flash Web files
/Cyclone.jpg     7867
free directory entries: 31
free file space: 55331

Telnet +> exit
```

Figure 166: Example telnet session to activate custom logo file

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

Procedure 43: Changing the URL of the logo hyperlink

1. In the editor of your choice, create a file named `top.html`, consisting of one line:

   `<a href="`***myurl***`">`

   where ***myurl*** is the desired URL, for example, http://www.Cyclonewireless.com.
2. Save and close the file as `top.html`.
3. Use an FTP (File Transfer Protocol) session to transfer this file to the module, as in the example session shown in Figure 165 on Page 454.
4. Use a telnet session and the addwebfile command to add the new file (top.html) to the file system, as in the example session shown in Figure 166.

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

If you ever want to restore the original logo and hyperlink in a module, perform the following steps.

Procedure 44: Returning a module to its original logo and hyperlink

1. Use a telnet session and the clearwebfile command to clear all custom files from the file system of the module, as in the example session shown in Figure 167

below.

```
>telnet ModuleIPAddress
/---------\
C A N O P Y

Last Mile Gear Broadband Wireless
Technology Center
(Copyright 2001, 2002 Last Mile Gear Inc.)

Login: root
Password: <password-if-configured>

Telnet +> lsweb
Flash Web files
Cyclone.jpg     7867
free directory entries: 31
free file space: 56468

Telnet +> clearwebfile
Telnet +> lsweb

Flash Web files
free directory entries: 32
free file space     64336 bytes

Telnet +> exit
```

Figure 167: Example telnet session to clear custom files

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

30 TOGGLING REMOTE ACCESS CAPABILITY

Based on your priorities for additional security and ease of network administration, you can deny or permit remote access individually to any AP, SM, or BH.

30.1 DENYING ALL REMOTE ACCESS

Wherever the No Remote Access feature is enabled by the following procedure, physical access to the module is required for

- any change in the configuration of the module.
- any software upgrade in the module.

Where additional security is more important that ease of network administration, you can disable all remote access to a module as follows.

Procedure 45: Denying all remote access

1. Insert the override plug into the RJ-11 GPS utility port of the module.
2. Power up or power cycle the module.
3. Access the web page http://169.254.1.1/lockconfig.html.
4. Click the check box.
5. Save the changes.
6. Reboot the module.
7. Remove the override plug.
   RESULT: No access to this module is possible through HTTP, SNMP, FTP, telnet, or over an RF link.

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

30.2 REINSTATING REMOTE ACCESS CAPABILITY

Where ease of network administration is more important than the additional security that the No Remote Access feature provides, this feature can be disabled as follows:

Procedure 46: Reinstating remote access capability

1. Insert the override plug into the RJ-11 GPS utility port of the module.
2. Power up or power cycle the module.
3. Access the web page http://169.254.1.1/lockconfig.html.
4. Click the check box to uncheck the field.
5. Save the changes.
6. Reboot the module.
7. Remove the override plug.
   RESULT: Access to this module is possible through HTTP, SNMP, FTP, telnet, or over an RF link.

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

31 SETTING UP A PROTOCOL ANALYZER ON YOUR CYCLONE NETWORK

Selection of protocol analyzer software and location for a protocol analyzer depend on both the network topology and the type of traffic to capture. However, the examples in this section are based on free-of-charge Ethereal software, which is available at http://ethereal.com/.

The equipment required to set up a protocol analyzer includes:

- 1 hub
- 1 laptop computer with protocol analyzer software installed
- 2 straight-through Ethernet cables
- 1 Cyclone power converter (ACPS110)

31.1 ANALYZING TRAFFIC AT AN SM

The IP address of the protocol analyzer laptop computer must match the IP addressing scheme of the SM. If the SM has DHCP enabled, then configure the laptop computer to automatically obtain an address. If DHCP is not enabled, then ensure that the laptop computer is configured with a static IP address in the same subnet as the SM.

The configuration for analyzing traffic at an SM is shown in Figure 168.

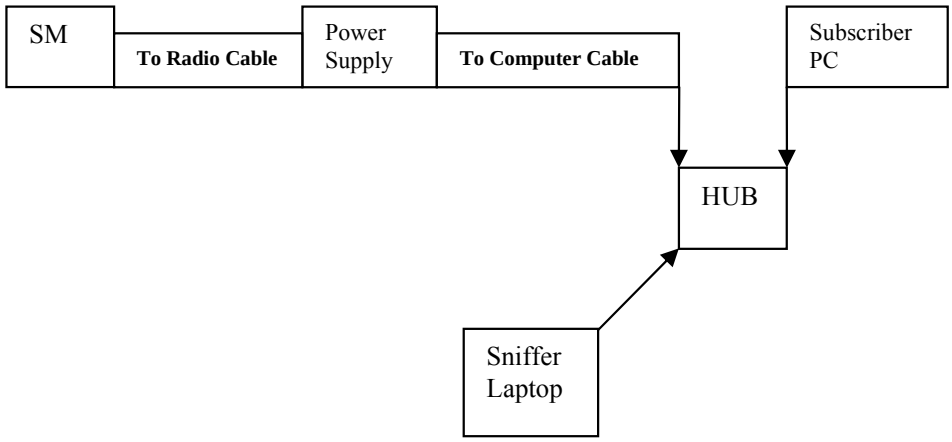

Figure 168: Protocol analysis at SM

31.2 ANALYZING TRAFFIC AT AN AP OR BH WITH NO CMM

The IP address of the protocol analyzer laptop computer must match the IP addressing scheme of the AP/BH. If the router is configured to be a DHCP server, then configure the laptop computer to automatically obtain an address. If DHCP is not enabled, then ensure that the laptop computer is configured with a static IP address in the same subnet as the AP/BH.

The configuration for analyzing traffic at an AP or BH that *is not* connected to a CMM is shown in Figure 169.

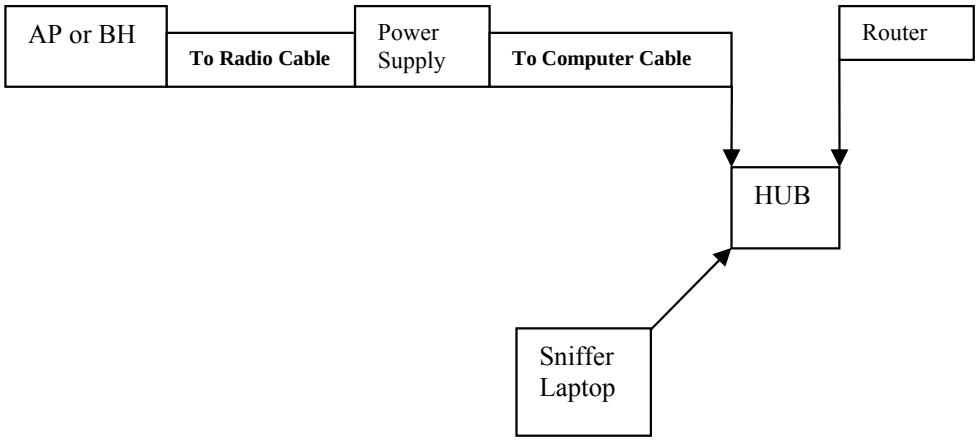

Figure 169: Protocol analysis at AP or BH not connected to a CMM

31.3 ANALYZING TRAFFIC AT AN AP OR BH WITH A CMM

The IP address of the protocol analyzer laptop computer must match the IP addressing scheme of the AP/BH. If the router is configured to be a DHCP server, then configure the laptop computer to automatically obtain an address. If DHCP is not enabled, ensure that the laptop computer is configured with a static IP address in the same subnet as the AP/BH.

Connect the hub to the J2 Ethernet to Switch of the port that is associated with the AP/BH. This example is of capturing traffic from AP/BH 111, which is connected to Port 1. The configuration for analyzing traffic at an AP or BH that is connected to a CMM is shown in Figure 170.

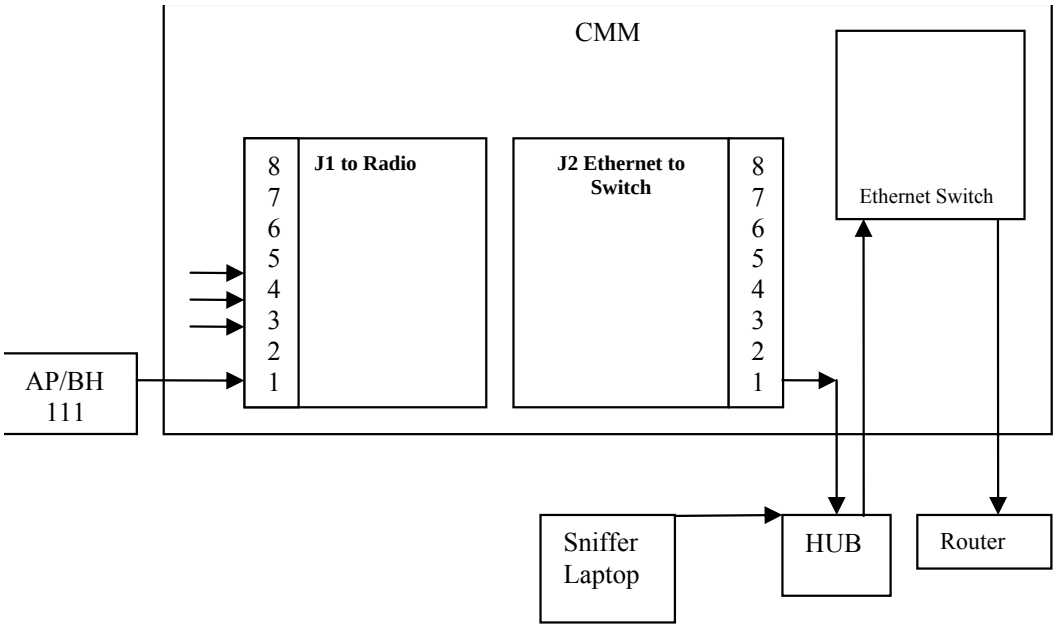

Figure 170: Protocol analysis at AP or BH connected to a CMM

31.4 EXAMPLE OF A PROTOCOL ANALYZER SETUP FOR AN SM

The following is an example of a network protocol analyzer setup using Ethereal® software to capture traffic at the SM level. The Ethereal network protocol analyzer has changed its name to Wireshark™, but functionality and use remains much the same. This example is based on the following assumptions:

- All required physical cabling has been completed.
- The hub, protocol analyzer laptop computer, and subscriber PC are successfully connected.
- The SM is connected
  - as shown in Figure 169 on Page 460.
  - to the subscriber PC and the AP.
- Ethereal software is operational on the laptop computer.

Although these procedures involve the SM, the only difference in the procedure for analyzing traffic on an AP or BH is the hub insertion point.

The IP Configuration screen of the example SM is shown in Figure 171.

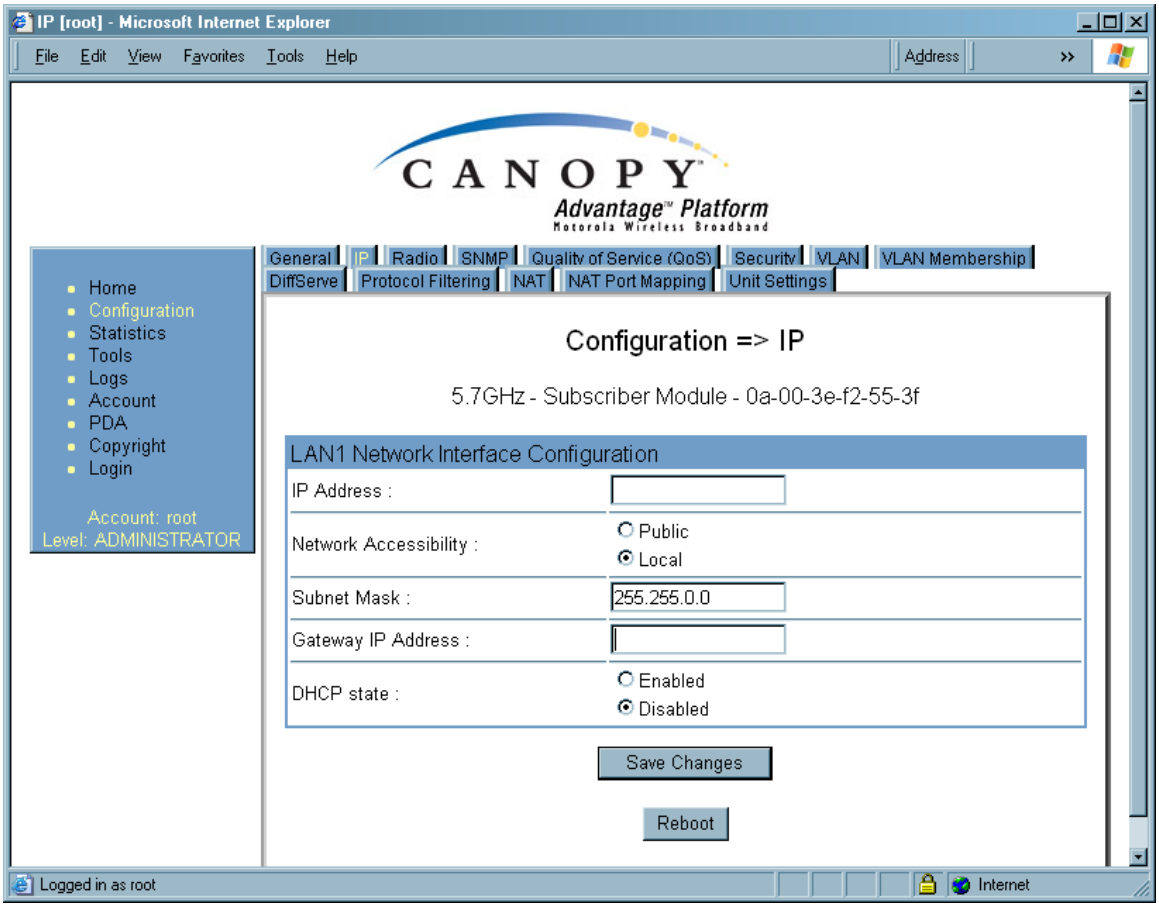

Figure 171: IP tab of SM with NAT disabled and local accessibility

Procedure 47: Setting up a protocol analyzer

1. Note the IP configuration of the SM.
2. Browse to **Start→My Network Places→Network and Dialup Connections**.
3. For **Local Area Connection**, select **Properties**.
   RESULT: The Local Area Connections Properties window opens, as shown in Figure 172.

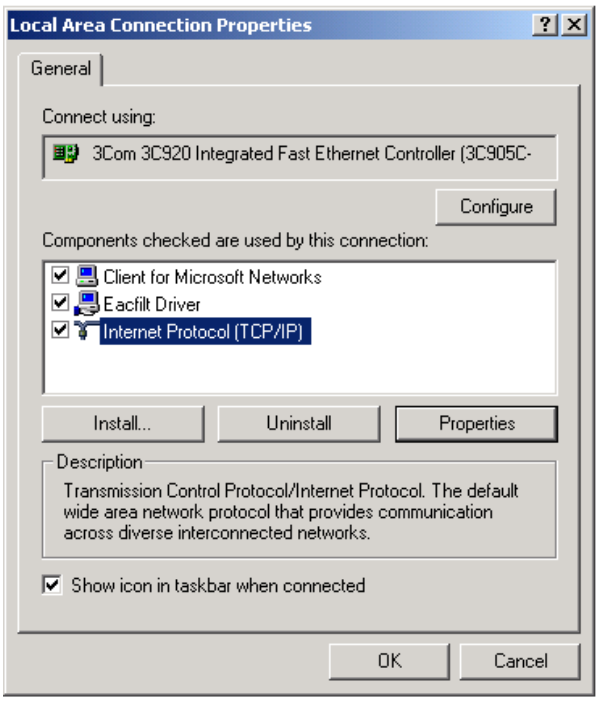

Figure 172: Local Area Connection Properties window

4. Select **Internet Protocol (TCP/IP)**.
5. Click the **Properties** button.
   RESULT: The Internet Protocol (TCP/IP) Properties window opens, as shown in Figure 173.

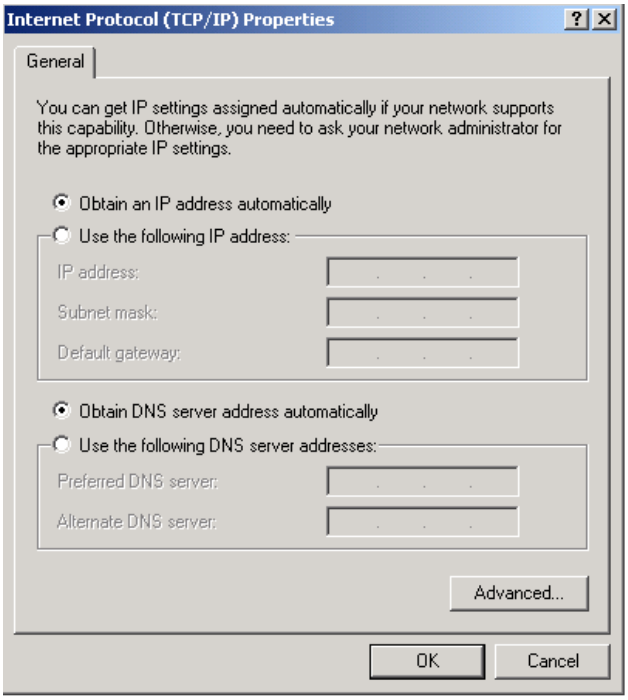

Figure 173: Internet Protocol (TCP/IP) Properties window

6. Unless you have a static IP address configured on the SM, select **Obtain an IP address automatically** for the protocol analyzer laptop computer, as shown in Figure 173.
7. If you have configured a static IP address on the SM, then
   a. select **Use the following IP address**.
   b. enter an IP address that is in the same subnet as the SM.
8. Click **OK**.
9. Open your web browser.
10. Enter the IP address of the SM.
    RESULT: The General Status tab of the SM opens, as shown in Figure 60 on Page 198.
11. If the General Status tab did not open, reconfigure how the laptop computer obtains an IP address.
12. Verify that you have connectivity from the laptop computer to the SM with the hub inserted.
13. Launch the protocol analyzer software on the laptop computer.
14. In the **Capture** menu, select **Start**.
    RESULT: The Ethereal Capture Options window opens, as shown in Figure 174.

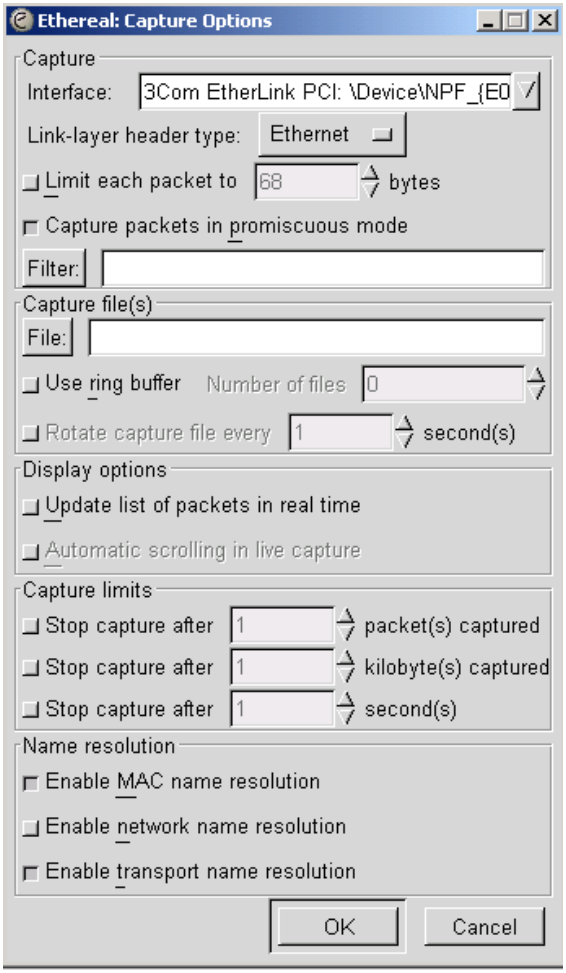

Figure 174: Ethereal Capture Options window

15. Ensure that the **Interface** field reflects the network interface card (NIC) that is used on the protocol analyzer laptop computer.
    NOTE: Although you can select filters based on specific types of traffic, all values are defaults in this example.
16. If you wish to select filters, select them now.
17. Click **OK**.
    RESULT: The Ethereal Capture window opens, as shown in Figure 175.

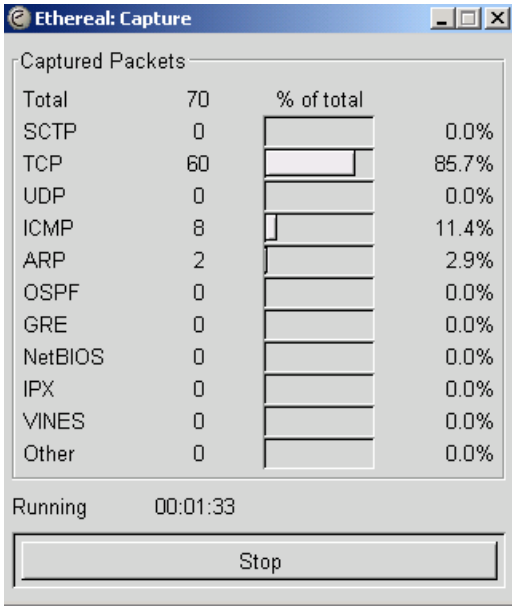

Figure 175: Ethereal Capture window

NOTE: This window graphically displays the types of packets (by percentage) that are being captured.

18. If all packet types are displayed with 0%, either
    - launch your Web browser on the subscriber PC for the IP address of the SM
    - ping the SM from the home PC.
19. If still all packet types are displayed with 0% (meaning that no traffic is being captured), reconfigure IP addressing until you can successfully see traffic captured on the laptop computer.
20. Whenever the desired number of packets have been captured, click **Stop**.
    RESULT: When you stop the packet capture, the <capture> - Ethereal window opens, as shown in Figure 176.

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

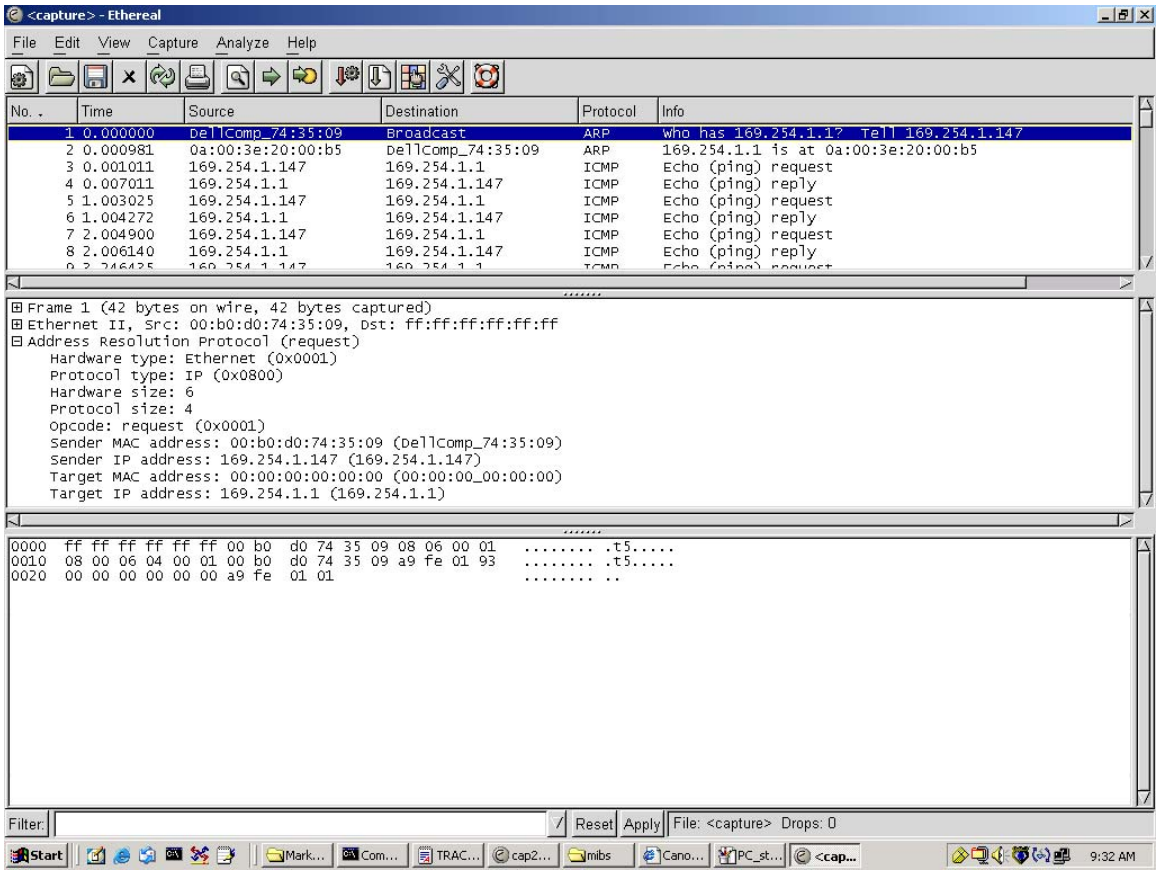

Figure 176: <capture> - Ethereal window, Packet 1 selected

This window has three panes:

- The top pane provides a sequenced summary of the packets captured and includes SRC/DEST address and type of protocol. What you select in this pane determines the additional information that is displayed in the lower two panes.
- The lower two panes facilitate drill-down into the packet that you selected in the top pane.

In this example, Packet 1 (a broadcast ARP request) was selected in the top pane. The lower two panes provide further details about Packet 1.

Another example is shown in Figure 177.

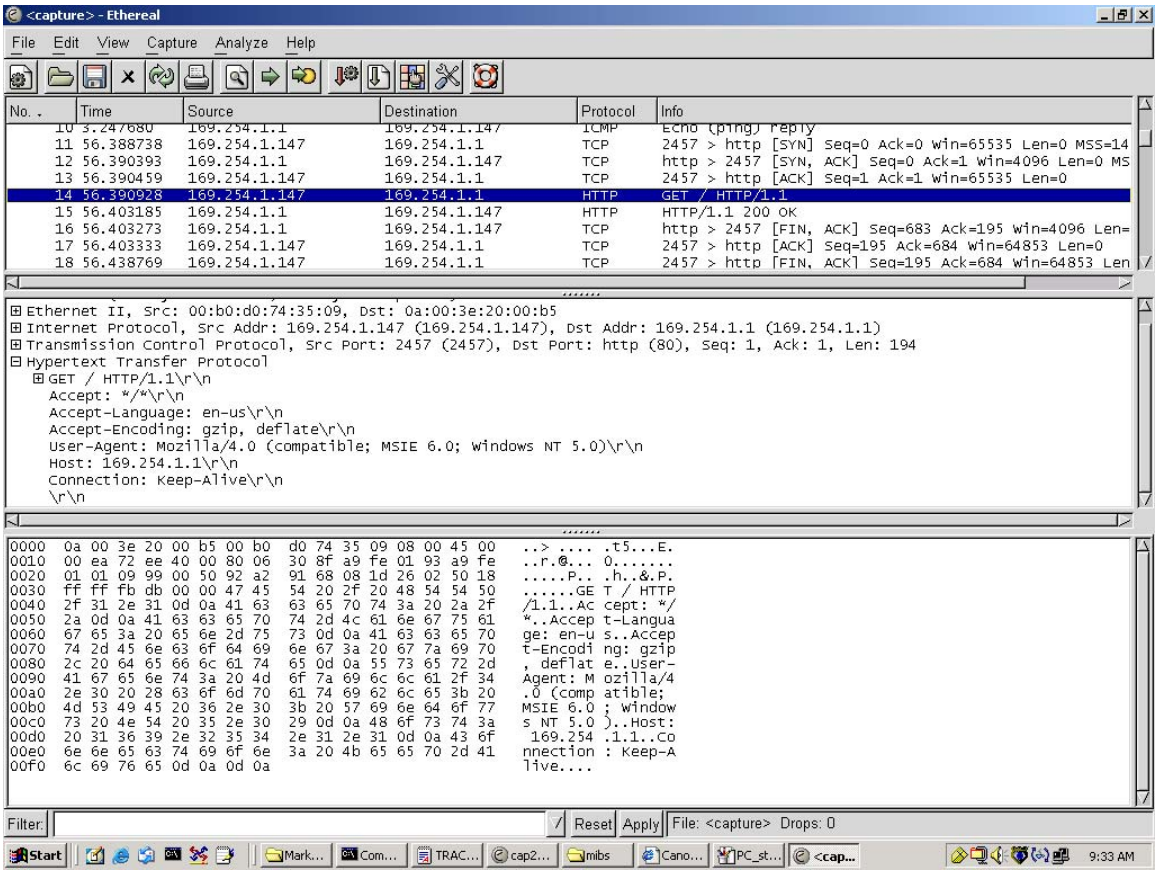

Figure 177: <capture> - Ethereal window, Packet 14 selected

In this second example, Packet 14 (protocol type HTTP) is selected in the top pane. The two lower panes provide further details about Packet 14.

32 TROUBLESHOOTING

32.1 GENERAL PLANNING FOR TROUBLESHOOTING

Effective troubleshooting depends in part on measures that you take before you experience trouble in your network. Cyclone recommends the following measures for each site:

1. Identify troubleshooting tools that are available at your site (such as a protocol analyzer).
2. Identify commands and other sources that can capture baseline data for the site. These may include
   - **`ping`**
   - **`tracert`** or **`traceroute`**
   - Link Capacity Test results
   - throughput data
   - Configuration tab captures
   - Status tab captures
   - session logs
3. Start a log for the site.
4. Include the following information in the log:
   - operating procedures
   - site-specific configuration records
   - network topology
   - software releases, boot versions, and FPGA firmware versions
   - types of hardware deployed
   - site-specific troubleshooting processes
   - escalation procedures
5. Capture baseline data into the log from the sources listed in Step 2.

32.2 GENERAL FAULT ISOLATION PROCESS

Effective troubleshooting also requires an effective fault isolation methodology that includes

- attempting to isolate the problem to the level of a system, subsystem, or link, such as
  - AP to SM
  - AP to CMM
  - AP to GPS
  - CMM to GPS
  - BHM to BHS
  - BHM to CMM
  - power

- researching Event Logs of the involved equipment. (See Interpreting Messages in the Event Log on Page 416.)
- answering the questions listed in the following section.
- reversing the last previous corrective attempt before proceeding to the next.
- performing only one corrective attempt at a time.

32.3 QUESTIONS TO HELP ISOLATE THE PROBLEM

When a problem occurs, attempt to answer the following questions:

1. What is the history of the problem?
   - Have we changed something recently?
   - Have we seen other symptoms before this?
2. How wide-spread is the symptom?
   - Is the problem on only a single SM? (If so, focus on that SM.)
   - Is the problem on multiple SMs? If so
     - is the problem on one AP in the cluster? (If so, focus on that AP)
     - is the problem on multiple, but not all, APs in the cluster? (If so, focus on those APs)
     - is the problem on all APs in the cluster? (If so, focus on the CMM and the GPS signal.)
3. Based on data in the Event Log (described in Interpreting Messages in the Event Log on Page 416)
   - does the problem correlate to External Hard Resets with no WatchDog timers? (If so, this indicates a loss of power. Correct your power problem.)
   - is intermittent connectivity indicated? (If so, verify your configuration, power level, jitter, cables and connections, and the speed duplex of both ends of the link).
   - does the problem correlate to loss-of-sync events?
4. Are connections made via *shielded* cables?
5. Does the GPS antenna have an *unobstructed* view of the entire horizon?

32.4 SECONDARY STEPS

After preliminary fault isolation through the above steps

1. check the Cyclone knowledge base (http://Last Mile Gear.Cyclonewireless.com/support/knowledge) to find whether other network operators have encountered a similar problem.
2. proceed to any appropriate set of diagnostic steps. These are organized as follows:
   - Module Has Lost or Does Not Establish Connectivity
   - NAT/DHCP-configured SM Has Lost or Does Not Establish Connectivity on Page 472
   - SM Does Not Register to an AP on Page 474
   - BHS Does Not Register to the BHM on Page 475
   - Module Has Lost or Does Not Gain Sync on Page 476

32.5 PROCEDURES FOR TROUBLESHOOTING

32.5.1 Module Has Lost or Does Not Establish Connectivity

To troubleshoot a loss of connectivity, perform the following steps.

Procedure 48: Troubleshooting loss of connectivity

1. Isolate the end user/SM from peripheral equipment and variables such as routers, switches, and firewalls.
2. Set up the minimal amount of equipment.
3. On each end of the link
   a. check the cables and connections.
   b. verify that the cable/connection scheme—straight-through or crossover—is correct.
   c. verify that the LED labeled LNK is green.
   d. access the General Status tab in the Home page of the module.
   e. verify that the SM is registered.
   f. verify that RSSI is 700 or higher.
   g. verify that jitter is reported as 9 or lower.
   h. access the IP tab in the Configuration page of the module.
   i. verify that IP addresses match and are in the same subnet.
4. On the SM end of the link
   a. verify that the PC that is connected to the SM is correctly configured to obtain an IP address through DHCP.
   b. execute **`ipconfig`**.
   c. verify that the PC has an assigned IP address.
5. On each end of the link
   a. access the General tab in the Configuration page of each module.
   b. verify that the setting for **Link Speeds** (or negotiation) matches that of the other module.
   c. access the Radio tab in the Configuration page of each module.
   d. verify that the **Radio Frequency Carrier** setting is checked in the **Custom Radio Frequency Scan Selection List**.
   e. verify that the **Color Code** setting matches that of the other module.
   f. access the browser LAN settings (for example, at **Tools→Internet Options→Connections→LAN Settings** in Internet Explorer).
   g. verify that none of the settings are selected.

h. access the Link Capacity Test tab in the Tools page of the module.

i. perform a link test. (See Procedure 40: Performing a Link Capacity Test on Page 439.)

j. verify that the link test results show efficiency greater than 90% in both the uplink and downlink (except as described under Comparing Efficiency in 1X Operation to Efficiency in 2X Operation on Page 135).

k. execute **`ping`**.

l. verify that no packet loss was experienced.

m. verify that response times are not significantly greater than

- 2.5 ms from BH to BH
- 4 ms from AP to SM
- 15 ms from SM to AP

n. replace any cables that you suspect may be causing the problem.

6. After connectivity has been re-established, reinstall network elements and variables that you removed in Step 1.

end of procedure

32.5.2 NAT/DHCP-configured SM Has Lost or Does Not Establish Connectivity

Before troubleshooting this problem, identify the NAT/DHCP configuration from the following list:

- NAT with DHCP Client and DHCP Server
- NAT with DHCP Client
- NAT with DHCP Server
- NAT without DHCP

To troubleshoot a loss of connectivity for an SM configured for NAT/DHCP, perform the following steps.

Procedure 49: Troubleshooting loss of connectivity for NAT/DHCP-configured SM

1. Isolate the end user/SM from peripheral equipment and variables such as routers, switches, and firewalls.
2. Set up the minimal amount of equipment.
3. On each end of the link
   a. check the cables and connections.
   b. verify that the cable/connection scheme—straight-through or crossover—is correct.
   c. verify that the LED labeled LNK is green.
4. At the SM
   a. access the NAT Table tab in the Logs web page.
   NOTE: An example of this tab is shown in Figure 178.

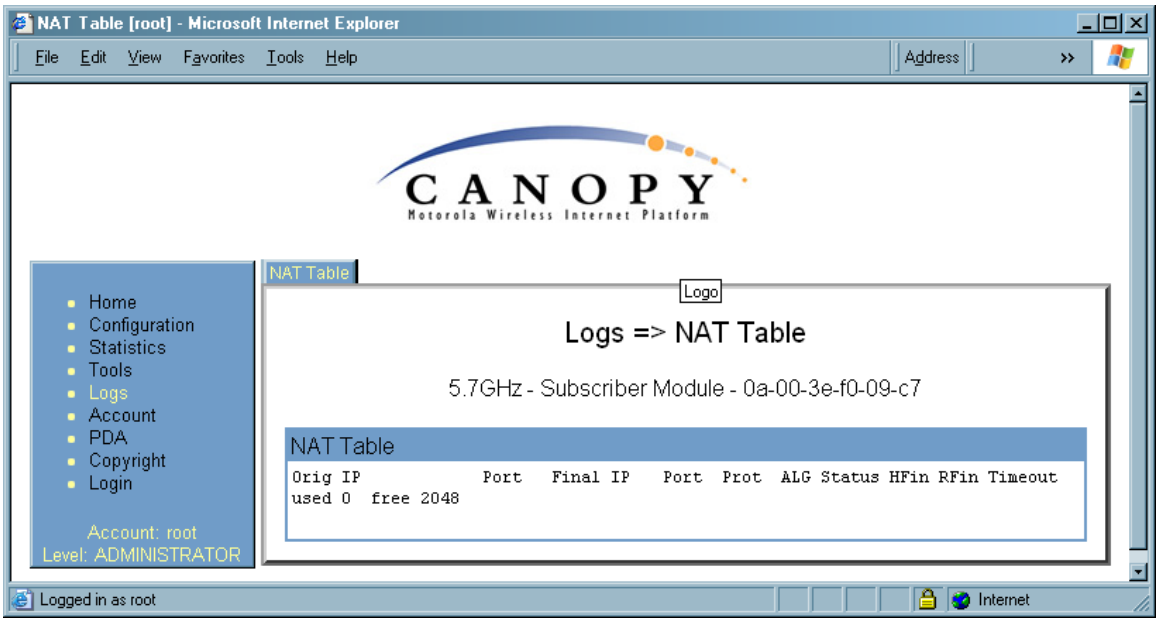

Figure 178: NAT Table tab of SM, example

b. verify that the correct NAT translations are listed.
RESULT: NAT is eliminated as a possible cause if these translations are correct.

5. If this SM is configured for NAT with DHCP, then at the SM
   a. execute **`ipconfig`**.
   b. verify that the PC has an assigned IP address.
   c. if the PC *does not* have an assigned IP address, then
      - enter **`ipconfig /release “Adapter Name”`**.
      - enter **`ipconfig /renew “Adapter Name”`**.
      - reboot the PC.
      - retreat to Step 5a.
   d. if the PC has an assigned IP address, then
      - access the NAT DHCP Statistics tab in the Statistics web page of the SM.
        NOTE: An example of this tab is shown in Figure 179.

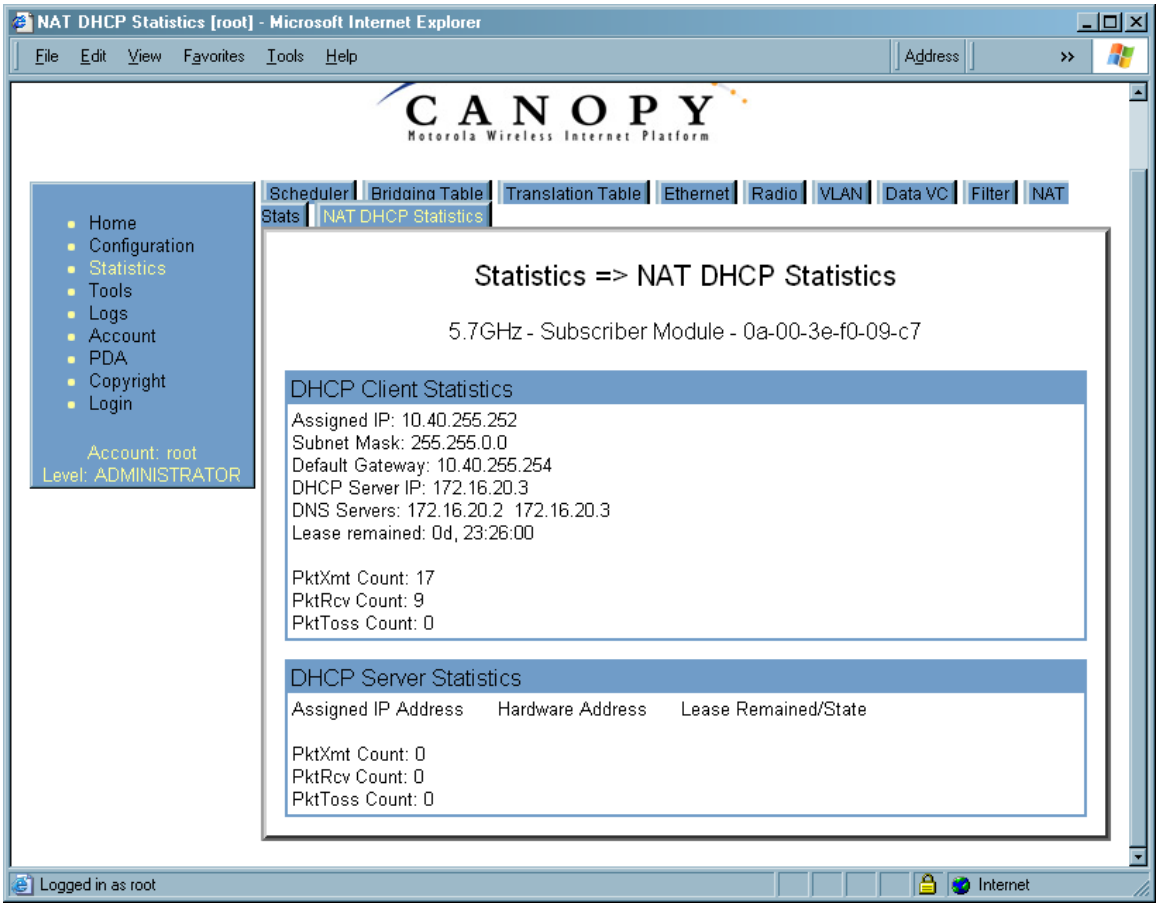

Figure 179: NAT DHCP Statistics tab of SM, example

- verify that DHCP is operating as configured.

6. After connectivity has been re-established, reinstall network elements and variables that you removed in Step 1.

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

32.5.3 SM Does Not Register to an AP

To troubleshoot an SM failing to register to an AP, perform the following steps.

Procedure 50: Troubleshooting SM failing to register to an AP

1. Access the Radio tab in the Configuration page of the SM.
2. Note the **Color Code** of the SM.
3. Access the Radio tab in the Configuration page of the AP.
4. Verify that the **Color Code** of the AP matches that of the SM.
5. Note the **Radio Frequency Carrier** of the AP.
6. Verify that the value of the **RF Frequency Carrier** of the AP is selected in the **Custom Radio Frequency Scan Selection List** parameter in the SM.

7. In the AP, verify that the **Max Range** parameter is set to a distance slightly greater than the distance between the AP and the furthest SM that must register to this AP.
8. Verify that a clear line of sight exists between the AP and the SM, and that no obstruction significantly penetrates the Fresnel zone of the attempted link. If these conditions are not established, then verify that the AP and SM are 900-MHz modules in close proximity to each other.
9. Access the General Status tab in the Home page of each module.
10. In the **Software Version** field, verify that both the AP and SM are of the same encryption scheme (AES or DES).
11. Remove the bottom cover of the SM to expose the LEDs.
12. Power cycle the SM.
    RESULT: Approximately 25 seconds after the power cycle, the green LED labeled LNK should light to indicate that the link has been established. If the orange LED labeled SYN is lit instead, then the SM is in Alignment mode because the SM failed to establish the link.
13. In this latter case, and if the SM has encountered no customer-inflicted damage, then request an RMA for the SM.

end of procedure

32.5.4 BHS Does Not Register to the BHM

To troubleshoot an BHS failing to register to the BHM, perform the following steps.

Procedure 51: Troubleshooting BHS failing to register to a BHM

1. Access the Radio tab in the Configuration page of the BHS.
2. Note the **Color Code** of the BHS.
3. Access the Radio tab in the Configuration page of the BHM.
4. Verify that the **Color Code** of the BHM matches that of the BHS.
5. Note the **Radio Frequency Carrier** of the BHM.
6. Verify that the value of the **RF Frequency Carrier** of the BHM is selected in the **Custom Radio Frequency Scan Selection List** parameter on the Configuration page of the BHS.
7. Verify that a clear line of sight exists between the BHM and BHS, and that no obstruction significantly penetrates the Fresnel zone of the attempted link.
8. Access the General Status tab in the Home page of each module.
9. In the **Software Version** field, verify that both the BHM and BHS are of the same encryption scheme (AES or DES).
10. Also in the Software Version field, verify that both the BHM and BHS are of the same modulation rate from the factory (BH20 or BH10).
11. Remove the bottom cover of the BHS to expose the LEDs.

12. Power cycle the BHS.
    RESULT: Approximately 25 seconds after the power cycle, the green LED labeled LNK should light to indicate that the link has been established. If the orange LED labeled SYN is lit instead, then the BHS is in Alignment mode because the BHS failed to establish the link. In this latter case, and if the BHS has encountered no customer-inflicted damage, then request an RMA for the BHS.

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

32.5.5 Module Has Lost or Does Not Gain Sync

To troubleshoot a loss of sync, perform the following steps.

Procedure 52: Troubleshooting loss of sync

1. Access the Event Log tab in the Home page of the SM.
   NOTE: An example of this tab is shown in Figure 180.

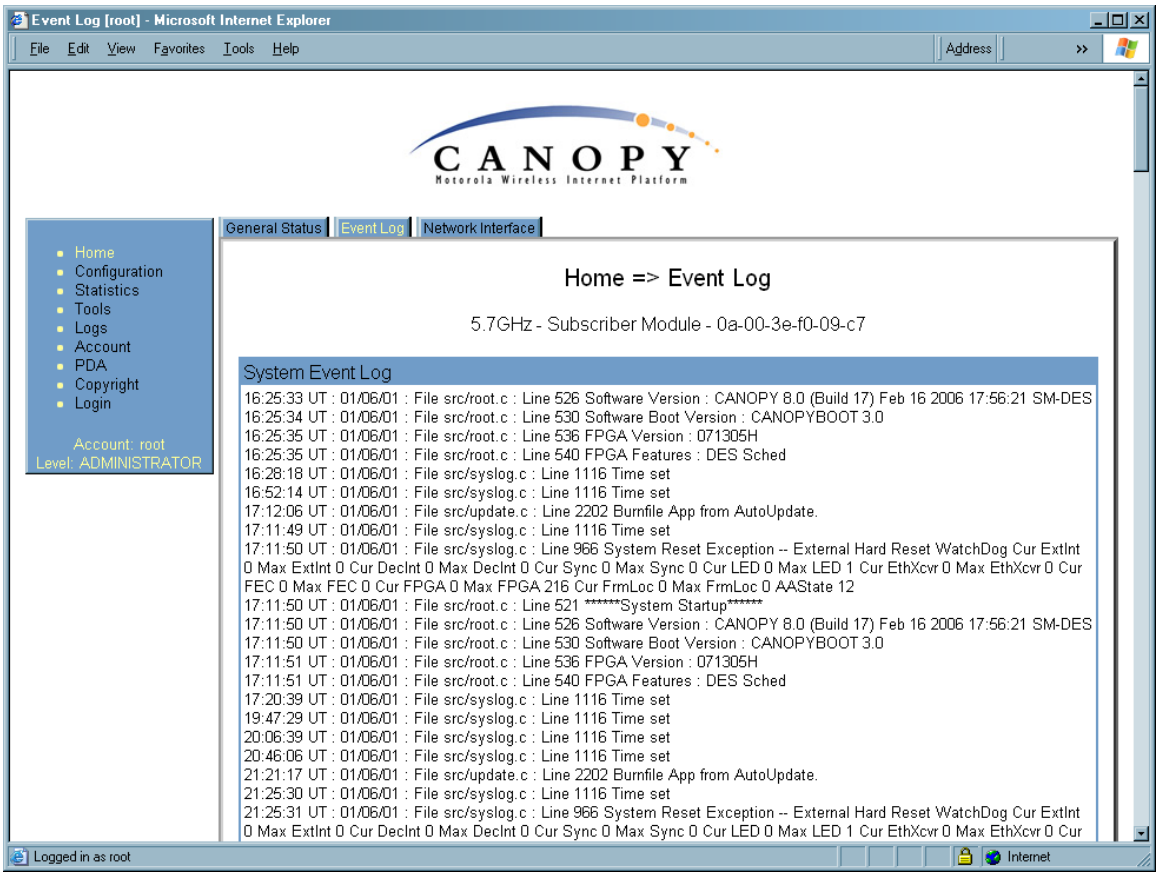

Figure 180: Event Log tab of SM, example

2. Check for messages with the following format:
   `RcvFrmNum =`
   `ExpFrmNum =`
   (See Table 63: Event Log messages for abnormal events on Page 419.)

3. If these messages are present, check the Event Log tab of another SM that is registered to the same AP for messages of the same type.
4. If the Event Log of this second SM *does not* contain these messages, then the fault is isolated to the first SM.
5. If the Event Log page of this second SM contains these messages, access the GPS Status page of the AP.
6. If the **Satellites Tracked** field in the GPS Status page of the AP indicates fewer than 4 or the **Pulse Status** field does not indicate Generating Sync, check the GPS Status page of another AP in the same AP cluster for these indicators.
7. If these indicators are present in the second AP
   a. verify that the GPS antenna still has an unobstructed view of the entire horizon.
   b. visually inspect the cable and connections between the GPS antenna and the CMM.
   c. if this cable is not shielded, replace the cable with shielded cable.
8. If these indicators *are not* present in the second AP
   a. visually inspect the cable and connections between the CMM and the AP antenna.
   b. if this cable is not shielded, replace the cable with shielded cable.

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

32.5.6 Module Does Not Establish Ethernet Connectivity

To troubleshoot a loss of Ethernet connectivity, perform the following steps.

Procedure 53: Troubleshooting loss of Ethernet connectivity

1. Verify that the connector crimps on the Ethernet cable are not loose.
2. Verify that the Ethernet cable is not damaged.
3. If the Ethernet cable connects the module to a network interface card (NIC), verify that the cable is pinned out as a straight-through cable.
4. If the Ethernet cable connects the module to a hub, switch, or router, verify that the cable is pinned out as a crossover cable.
5. Verify that the Ethernet port to which the cable connects the module is set to auto-negotiate speed.
6. Power cycle the module.
   RESULT: Approximately 25 seconds after the power cycle, the green LED labeled LNK should light to indicate that the link has been established. If the orange LED labeled SYN is lit instead, then the module is in Alignment mode because the module failed to establish the link.
7. In this latter case, and if the module has encountered no customer-inflicted damage, then request an RMA for the module.

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

32.5.7 Module Does Not Power Up

To troubleshoot the failure of a module to power up, perform the following steps.

Procedure 54: Troubleshooting failure to power up

1. Verify that the connector crimps on the Ethernet cable are not loose.
2. Verify that the Ethernet cable is not damaged.
3. Verify that the cable is wired and pinned out according to the specifications provided under Wiring Connectors on Page 182.
4. Remove the cover of the module to expose the components on the printed wiring board.
5. Find the Ethernet transformer, which is labeled with either the name Halo or the name Pulse.
6. Verify that the Ethernet transformer does not show damage that would have been caused by improper cabling. (You can recognize damage as the top of the transformer being no longer smooth. The transformer in the following picture is damaged and is ineligible for an RMA.)

7. Connect the power supply to a known good Cyclone module via a known good Ethernet cable.
8. Attempt to power up the known good module and
   - if the known good module fails to power up, request an RMA for the power supply.
   - if the known good module powers up, return to the module that does not power up.
9. Reconnect the power supply to the failing module.
10. Connect the power supply to a power source.
11. Verify that the red LED labeled PWR lights.
12. If this LED *does not* light, and the module has not been powered up since the last previous FPGA firmware upgrade was performed on the module, then request an RMA for the module.

end of procedure

32.5.8 Power Supply Does Not Produce Power

To troubleshoot the failure of a power supply to produce power, perform the following steps.

Procedure 55: Troubleshooting failure of power supply to produce power

1. Verify that the connector crimps on the Ethernet cable are not loose.
2. Verify that the Ethernet cable is not damaged.

3. Verify that the cable is wired and pinned out according to the specifications provided under Wiring Connectors on Page 182.
4. Connect the power supply to a known good Cyclone module via a known good Ethernet cable.
5. Attempt to power up the known good module.
6. If the known good module fails to power up, request an RMA for the power supply.

end of procedure

32.5.9 CMM2 Does Not Power Up

To troubleshoot a malfunctioning CMM2, perform the following steps.

Procedure 56: Troubleshooting CMM2 that malfunctions

1. Verify that the 115-/230-V switch (in the lower right-hand corner of the CMM2) is in the correct position for the power source. (See Figure 123 on Page 341.) Applying power when this switch is in the wrong position can damage the CMM2 and will render it ineligible for an RMA.
2. Verify that the electrical source to the CMM2 meets Cyclone specifications. See Table 18 on Page 72.
3. Verify that the electrical source is connected to the CMM2 at the proper connection point. (See Figure 125 on Page 344.)
4. Verify that the fuse is operational.
5. Verify that the fuse is properly seated in the receptacle.
6. Attempt to power up the CMM2.
7. If the power indicator on the interconnect board of the CMM2 fails to light when power is applied to the CMM2, request an RMA for the CMM2.

end of procedure

32.5.10 CMM2 Does Not Pass Proper GPS Sync to Connected Modules

If the Event Log tabs in all connected modules contain `Loss of GPS Sync Pulse` messages, perform the following steps.

Procedure 57: Troubleshooting CMM2 not passing sync

1. Verify that the GPS antenna has an unobstructed view of the entire horizon.
2. Verify that the GPS coaxial cable meets specifications.
3. Verify that the GPS sync cable meets specifications for wiring and length.
4. If the web pages of connected modules indicate any of the following, then find and eliminate the source of noise that is being coupled into the GPS sync cable:
   - In the GPS Status page
     - anomalous number of **Satellites Tracked** (greater than 12, for example)
     - incorrect reported **Latitude** and/or **Longitude** of the antenna
   - In the Event Log page
     - garbled GPS messages
     - large number of `Acquired GPS Sync Pulse` messages

5. If these efforts fail to resolve the problem, then request an RMA for the CMM2.

end of procedure

32.5.11 Module Software Cannot be Upgraded

If your attempt to upgrade the software of a module fails, perform the following steps.

Procedure 58: Troubleshooting an unsuccessful software upgrade

1. Download the latest issue of the target release and the associated release notes.
2. Compare the files used in the failed attempt to the newly downloaded software.
3. Compare the procedure used in the failed attempt to the procedure in the newly downloaded release notes.
4. If these comparisons reveal a difference, retry the upgrade, this time with the newer file or newer procedure.
5. If, during attempts to upgrade the FPGA firmware, the following message is repeatable, then request an RMA for the module:

   ```
   Error code 6, unrecognized device
   ```

end of procedure

32.5.12 Module Functions Properly, Except Web Interface Became Inaccessible

If a module continues to pass traffic, and the telnet and SNMP interfaces to the module continue to function, but the web interface to the module does not display, perform the following steps.

Procedure 59: Restoring the web interface to a module

1. Enter **`telnet`** ***`DottedIPAddress`***.
   RESULT: A telnet session to the module is invoked.
2. At the `Login` prompt, enter **`root`**.
3. At the `Password` prompt, enter ***`PasswordIfConfigured`***.
4. At the `Telnet +>` prompt, enter **`reset`**.
   RESULT: The web interface is accessible again, and this telnet connection is closed.

end of procedure

33 OBTAINING TECHNICAL SUPPORT

NOTE:
The contact information for Cyclone Technical Support staff is included at the end of this section (on Page 485). However, in most cases, you should follow the procedure of this section before you contact them.

To get information or assistance as soon as possible for problems that you encounter, use the following sequence of actions:

1. Search this document, the user guides of products that are supported by dedicated documents, and the software release notes of supported releases
   a. in the Table of Contents for the topic.
   b. in the Adobe Reader® search capability for keywords that apply.[8]
2. Visit http://Last Mile Gear.Cyclonewireless.com/support/knowledge to view the Cyclone Knowledge Base.
3. Ask your Cyclone products supplier to help.
4. View and analyze event logs, error messages, and debug messages to help isolate the problem.
5. Check release notes and verify that all of your Cyclone equipment is on the correct software release.
6. Verify that the Cyclone configuration files match the last known good (baseline) Cyclone configuration files captured in the site log book.
7. Verify connectivity (physical cabling).
8. At the SM level, minimize your network configuration (remove home network devices to help isolate problem).
9. Perform the site verification checklist.
10. Use Table 65 (two pages) as a job aid to collect basic site information for technical support to use.

[8] Reader is a registered trademark of Adobe Systems, Incorporated.

Table 65: Basic site information for technical support

Call Log Number:	Company:	Location:
Problem Type:	Site Contact:	Site Phone:
Call Severity (Select One): 1- Urgent-Customer Svc Down 2- Serious- Customer Svc Impacted 3- Non-Critical/General Inquiry	Open Date:	Close Date:
Product Types Involved: (ID the product type) 2400 SM/AP/BHM/BHS 5200 ER /BHM/BHS 5200 SM/AP/BHM/BHS 5700 SM/AP/BHM/BHS 1008CK 300SS ACPS110	MAC Addresses:	IP Addresses:
Software Releases:	Boot Versions:	FPGA Versions:
Authentication ?: Yes/No Type:	Is the customer using shielded cables? Yes/No	Remote Access Method: IP Address:

Network Scenario for this issue: (ID those that apply) SM to Subscriber PC Yes/No SM to AP (Point to Multipoint) Yes/No BHM to BHS (Point to Point) Yes/No 20Meg or 10Meg backhaul Yes/No	Link Distance: dBm= Jitter=	Reflectors in use: Yes/No
NAT/DHCP Scenario: NAT Disabled Yes/No NAT with DHCP Client and DHCP Server Yes/No NAT with DHCP Client Yes/No NAT with DHCP Server Yes/No NAT with no DHCP Yes/No	Problem Description: New Install: Yes/No	NAT/DHCP Scenario: NAT Disabled Yes/No NAT with DHCP Client and DHCP Server Yes/No NAT with DHCP Client Yes/No NAT with DHCP Server Yes/No NAT with no DHCP Yes/No

11. Save your basic site information as file `Site_Info`.
12. From among Figure 28 on Page 103, Figure 29 on Page 104, and Figure 30 on Page 104, select the basic network topology diagram that most closely matches your network configuration.
13. If you selected Figure 28.
    a. Indicate how many APs are in each cluster.
    b. Indicate how many AP clusters are deployed (and what types).
    c. Include the IP addresses.
    d. Indicate the frequency for each sector.
    e. Indicate the type of synchronization.
    f. Indicate how much separation exists between clusters.
    g. For each AP collect the following additional information:
       - Sector number:
       - SW release:
       - Frequency:
       - Color code:

- IP address:
- Downlink/uplink ratio:
- Max range:
- Bridge entry timeout:
- Number of subscribers:
- Method of synchronization:

14. If you selected Figure 29
    a. Indicate how many APs are in each cluster.
    b. Indicate how many AP clusters are deployed (and what types).
    c. Indicate how many BH links are configured.
    d. Include the IP addresses.
    e. Indicate the frequency for each sector.
    f. Indicate the type of synchronization.
    g. Indicate how much separation exists between clusters and BHs.
    h. Indicate the types of BH links (10-Mbps or 20-Mbps).
    i. Distances of links.
    j. Frequency used by each BH.
    k. For each AP and BHM, collect the following additional information:
        - Sector number:
        - SW release:
        - Frequency:
        - Color code:
        - IP address:
        - Downlink/uplink ratio:
        - Max range:
        - Bridge entry timeout:
        - Number of subscribers:
        - Method of synchronization:
15. If you selected Figure 30, collect the following additional information:
    - Sector number:
    - SW release:
    - Frequency:
    - Color code:
    - IP address:
    - Downlink/uplink ratio:
    - Max range:
    - Bridge entry timeout:
    - Number of subscribers:
    - Method of synchronization:
16. Add any details that are not present in the generic diagram that you selected.
17. Save your diagram as file `Net_Diagram`.

18. Capture screens from the following web pages of affected modules:
    - Home page Status tabs as files *SM/AP/BHM/BHS*_Status*Tabname*.*gif*
    - Configuration page tabs as files *SM/AP/BHM/BHS*_Config*Tabname*.*gif*
    - Home page Event Log as file *SM/AP/BHM/BHS*_Events.*gif*
    - Tools page Link Capacity Test tab (with link test results) as file *SM/AP/BHM/BHS*_LinkTST.*gif*
    - Statistics page Radio tab as file *SM/AP/BHM/BHS*_RFstats.*gif*
19. For any affected SM or BHS, capture the Tools page AP Evaluation tab as file *SM/BHS*_APEval.*gif*.
20. For any affected SM that has NAT/DHCP enabled, capture screens from the following additional web pages:
    - Configuration page NAT tab as file *SM*_Natconfig.*gif*
    - Configuration page NAT Port Mapping tab as file SM_NatPortmap.*gif*
    - Logs page NAT Table tab as file *SM*_NatTable.*gif*
    - Statistics page NAT Stats tab as file *SM*_NatStats.*gif*
    - Statistics page Translation Table tab as file *SM*_ArpStats.*gif*
    - Statistics page NAT DHCP Statistics tab as file *SM*_DhcpStats.*gif*

    Also capture the Windows IP Configuration screen as file *SM* _WindowsIP.*gif*.
21. Escalate the problem to Cyclone systems Technical Support (or another technical support organization that has been designated for you) as follows:
    a. Start e-mail to technical-support@Cyclonewirelessless.com. In this email
        - Describe the problem.
        - Describe the history of the problem.
        - List your attempts to solve the problem.
        - Attach the above files.
        - List the files that you are attaching.
    b. Send the email.
    c. Call 1 888 605 2552 (or +1 217 824 9742).

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

34 GETTING WARRANTY ASSISTANCE

For warranty assistance, contact your reseller or distributor for the process.

REFERENCE INFORMATION

35 ADMINISTERING MODULES THROUGH TELNET INTERFACE

In the telnet administrative interface to a module, the Cyclone platform supports the commands defined in Table 66. Many of these are not needed with CNUT.

Table 66: Supported telnet commands for module administration

Command	System help Definition	Notes
addwebfile	Add a custom web file	Syntax: **addwebfile *filename***. Copies the custom web file *filename* to non-volatile memory.
burnfile	Burn flash from file	Syntax: **burnfile *filename***. Updates the CPU firmware with a new image. User the image contained in *filename* if *filename* is provided. If provided, *filename* must match the module type (for example, SMboot.bin for a Subscriber Module or APboot.bin for an Access Point Module).
cat	Concatenate and display.	Syntax: **cat *filename***. Displays the contents of *filename*.
clearsyslog	Clear the system event log	Syntax: **clearsyslog**. Clears the system event log.
clearwebfile	Clear all custom web files	Syntax: **clearwebfile**. Deletes all *custom* web files.
exit	Exit from telnet session	Syntax: **exit**. Terminates the telnet interface session.
fpga_conf	Update FPGA program	Syntax: **fpga_conf**. Forces a module to perform a hard (FPGA and CPU) reset. (See reset.)
ftp	File transfer application	Syntax: **ftp**. Launches the ftp client application on the module.
help	Display command line function help	Syntax: **help**. Displays a list of available telnet commands and a brief description of each.
jbi	Update FPGA program	Syntax: **jbi –aprogram *file.jbc***. Updates the FPGA firmware with the new image contained in *file.jbc*.
ls	List the contents of a directory	Syntax: **ls**. Lists the file names of all files in the directory. Syntax: **ls –l**. Displays additional information, such as the sizes and dates of the files.
lsweb	List Flash Web files	Syntax: **lsweb**. Lists the file names of the saved custom web files.

Command	System help Definition	Notes
ping	Send ICMP ECHO_REQUEST packets to network hosts	Syntax: **ping *IPaddress***. Sends an ICMP ECHO_REQUEST to *IPaddress* and waits for a response. If a response is received, the system returns *IPaddress* is alive. If no response is received, the system returns no answer from *IPaddress*.
reset	Reboot the unit	Syntax: **reset**. Forces the module to perform a hard (FPGA and CPU) module reset. (See **fpga_conf**.)
rm	Remove (unlink) files	Syntax: **rm *filename***. Remove *filename*.
syslog	Display system event log: syslog <optional filename>	Syntax: **syslog**. Displays the contents of the system log. Syntax: **syslog *filename***. Saves the contents of the system log to *filename*. Caution: overwrites *filename* if it already exists.
telnet	Telnet application	Syntax: **telnet *hostIPaddress***. Launches the telnet client application on the Cyclone module.
tftp	tftp application	Syntax: **tftp *hostIPaddress***. Launches the tftp client application on the Cyclone module.
update	Enable automatic SM code updating	Syntax: **update *actionlist.txt***. Enables the automated update procedure that *actionlist.txt* specifies. (Supported for only the Access Point Module.)
updateoff	Disable automatic SM code updating	Syntax: **updateoff**. Disables the automated update procedure.
version	Display the software version string	Syntax: **version**. Displays the module version string, which contains the software/firmware/hardware versions, the module type, and the operating frequency.

36 REGULATORY AND LEGAL NOTICES

36.1 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.

36.2 NATIONAL AND REGIONAL REGULATORY NOTICES

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

This device complies with Part 15 of the US FCC Rules and Regulations. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B 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.

FCC IDs and the specific configurations covered are listed in Table 67.

Table 67: US FCC IDs and Industry Canada Certification Numbers and Covered Configurations

FCC ID	Industry Canada Cert Number	Frequencies	Module Families	Antenna or Reflector	Maximum Transmitter Output Power
ABZ89FC5809	109W-9000	8 MHz channels, centered on 906-924 MHz in 1 MHz increments (within the 902-928 MHz ISM band)	900 SM, AP	12 dBi Cyclone integrated antenna	24 dBm (250 mW)
				10 dBi Maxrad Model # Z1681, flat panel	26 dBm (400 mW)
				10 dBi Mars Model # MA-IS91-T2, flat panel	26 dBm (400 mW)
				10 dBi MTI Model #MT-2630003/N, flat panel	26 dBm (400 mW)
ABZ89FC5808	109W-2400	20 MHz channels, centered on 2415-2457.5 MHz in 2.5 MHz increments (within the 2400-2483.5 MHz ISM band)	2400 BH, SM, AP	8 dBi internal	25 dBm (340 mW)
			2400 BH, SM	8 dBi internal + 11 dB reflector	25 dBm (340 mW)
ABZ89FC3789	109W-5200	20 MHz channels, centered on 5275-5325 MHz in 5 MHz increments (within the 5250-5350 MHz U-NII band)	5200 BH, SM, AP	7 dBi internal	23 dBm (200 mW)
			5200 BH or SM, only P10 Modules	7 dBi internal + 18 dB reflector	5 dBm (3.2 mW)
				7 dBi internal + 9 dB lens	14 dBm
ABZ89FC5807	109W-5210	20 MHz channels, centered on 5275-5325 MHz in 5 MHz increments (within the 5250-5350 MHz U-NII band)	5210 BH	7 dBi internal + 18 dB reflector	5 dBm (3.2 mW)
ABZ89FT7623	---	20 MHz channels, centered on 5495-5705 MHz in 5 MHz increments (within the 5470-5725 MHz U-NII band)	5400 BH, SM, AP	7 dBi internal	23 dBm (200 mW)
			5400 BH, SM	7 dBi internal + 18 dB reflector	5 dBm (3.2 mW)
				7 dBi internal + 9 dB lens	14 dBm

FCC ID	Industry Canada Cert Number	Frequencies	Module Families	Antenna or Reflector	Maximum Transmitter Output Power
---	109W-5400	20 MHz channels, centered on 5495-5575 and 5675-5705 MHz in 5 MHz increments (within the 5470-5725 MHz U-NII band with 5600-5650 MHz excluded)	5400 BH, SM, AP	7 dBi internal	23 dBm (200 mW)
			5400 BH, SM	7 dBi internal + 18 dB reflector	5 dBm (3.2 mW)
				7 dBi internal + 9 dB lens	14 dBm
ABZ89FC5804	109W-5700	20 MHz channels, centered on 5735-5840 MHz in 5 MHz increments (within the 5725-5850 MHz ISM band)	5700 BH, SM, AP	7 dBi internal	23 dBm (200 mW)
			5700 BH, SM	7 dBi internal + 18 dB reflector	23 dBm (200 mW)
				7 dBi internal + 10 di lens	23 dBm (200 mW)
ABZ89FT7629	---	10 MHz channels, centered on 5476-5719 in 0.5 MHz increments (within the 5470-5725 MHz U-NII band)	5440 AP	17 dBi connectorized antenna (60° x 5° 3 dB beam width)	10 dBm
			5440 SM	17 dBi integrated antenna (18° x 18° 3 dB beam width)	10 dBm

36.2.2 Industry Canada (IC) Notification

This device complies with RSS-210 of Industry Canada. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation.

Users should be cautioned to take note that in Canada high power radars are allocated as primary users (meaning they have priority) of 5250 – 5350 MHz and 5650 – 5850 MHz and these radars could cause interference and/or damage to license-exempt local area networks (LELAN).

This equipment has been tested and found to comply with the limits for a Class B 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.

Industry Canada Certification Numbers and the specific configurations covered are listed in Table 67.

This device has been designed to operate with the antennas listed in Table 67 and having a maximum gain as shown in Table 67. Antennas not included or having a gain greater than as shown in Table 67 are strictly prohibited from use with this device. Required antenna impedance is 50 ohms.

36.2.3 Regulatory Requirements for CEPT Member States (www.cept.org)

When operated in accordance with the instructions for use, Last Mile Gear Cyclone Wireless equipment operating in the 2.4 and 5.4 GHz bands is compliant with CEPT Recommendation 70-03 Annex 3 for Wideband Data Transmission and HIPERLANs. For compliant operation in the 2.4 GHz band, the transmit power (EIRP) from the built-in patch antenna and any associated reflector dish shall be no more than 100mW (20dBm). For compliant operation in the 5.4 GHz band, the transmit power (EIRP) from the built-in patch antenna and any associated reflector dish shall be no more than 1 W (30 dBm).

The following countries have completely implemented CEPT Recommendation 70-03 Annex 3A (2.4 GHz band):

- EU & EFTA countries**:** Austria, Belgium, Denmark, Spain, Finland, Germany, Greece, Iceland, Italy, Ireland, Liechtenstein, Luxembourg, Netherlands, Norway, Portugal, Switzerland, Sweden, UK
- New EU member states**:** Bulgaria, Czech Republic, Cyprus, Estonia, Hungary, Lithuania, Latvia, Malta, Poland, Slovenia, Slovakia
- Other non-EU & EFTA countries: Bosnia and Herzegovina, Turkey

The following countries have a limited implementation of CEPT Recommendation 70-03 Annex 3A:

- France **–** Outdoor operation at 100mW is only permitted in the frequency band 2400 to 2454 MHz;
  - Any outdoor operation in the band 2454 to 2483.5MHz shall not exceed 10mW (10dBm);
  - Indoor operation at 100mW (20dBm) is permitted across the band 2400 to 2483.5 MHz
- French Overseas Territories:
  - Guadeloupe, Martinique, St Pierre et Miquelon, Mayotte – 100mW indoor & outdoor is allowed
  - Réunion and Guyana – 100mW indoor, no operation outdoor in the band 2400 to 2420MHz
- Italy – If used outside own premises, general authorization required

- Luxembourg - General authorization required for public service
- Romania – Individual license required. T/R 22-06 not implemented

Last Mile Gear Cyclone Radios operating in the 2400 to 2483.5MHz band are categorized as “Class 2” devices within the EU and are marked with the class identifier symbol ⓘ, denoting that national restrictions apply (for example, France). The French restriction in the 2.4 GHz band will be removed in 2011.

This 2.4 GHz equipment is “CE” marked CE ⓘ to show compliance with the European Radio & Telecommunications Terminal Equipment (R&TTE) directive 1999/5/EC. The relevant Declaration of Conformity can be found at http://Last Mile Gear.Cyclonewireless.com/doc.php.

Where necessary, the end user is responsible for obtaining any National licenses required to operate this product and these must be obtained before using the product in any particular country. However, for CEPT member states, 2.4 GHz Wideband Data Transmission equipment has been designated exempt from individual licensing under decision ERC/DEC(01)07. For EU member states, RLAN equipment in both the 2.4 & 5.4GHz bands is exempt from individual licensing under Commission Recommendation 2003/203/EC. Contact the appropriate national administrations for details on the conditions of use for the bands in question and any exceptions that might apply. Also see www.ero.dk for further information.

Last Mile Gear Cyclone Radio equipment operating in the 5470 to 5725 MHz band are categorized as “Class 1” devices within the EU in accordance with ECC DEC(04)08 and are “CE” marked CE to show compliance with the European Radio & Telecommunications Terminal Equipment (R&TTE) directive 1999/5/EC. The relevant Declaration of Conformity can be found at http://Last Mile Gear.Cyclonewireless.com/doc.php.

A European Commission decision, implemented by Member States on 31 October 2005, makes the frequency band 5470-5725 MHz available in all EU Member States for wireless access systems. Under this decision, the designation of Cyclone 5.4GHz products become “Class 1 devices” and these do not require notification under article 6, section 4 of the R&TTE Directive. Consequently, these 5.4GHz products are only marked with the CE symbol and may be used in any member state.

For further details, see http://europa.eu.int/information_society/policy/radio_spectrum/ref_documents/index_en.htm

36.2.4 European Union Notification for 5.7 GHz Product

The 5.7 GHz connectorized product is a two-way radio transceiver suitable for use in Broadband Wireless Access System (WAS), Radio Local Area Network (RLAN), or Fixed Wireless Access (FWA) systems. It is a Class 2 device and uses operating frequencies that are not harmonized throughout the EU member states. The operator is responsible for obtaining any national licenses required to operate this product and these must be obtained before using the product in any particular country.

This equipment is marked CE ⓘ 0977 to show compliance with the European R&TTE directive 1999/5/EC.

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

36.2.5 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.

36.2.6 EU Declaration of Conformity for RoHS Compliance

Last Mile Gear hereby, declares that these Last Mile Gear 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.Cyclonewireless.com/doc.php.

36.2.7 UK Notification

The 5.7 GHz connectorized product has been notified for operation in the UK, and when operated in accordance with instructions for use it is compliant with UK Interface Requirement IR2007. For UK use, installations must conform to the requirements of IR2007 in terms of EIRP spectral density against elevation profile above the local horizon in order to protect Fixed Satellite Services. The frequency range 5795-5815 MHz is assigned to Road Transport & Traffic Telematics (RTTT) in the U.K. and shall not be used by FWA systems in order to protect RTTT devices. UK licensing specifies that radiolocation services shall be protected by a Dynamic Frequency Selection (DFS) mechanism to prevent co-channel operation in the presence of radar signals.

36.2.8 Belgium Notification

Belgium national restrictions in the 2.4 GHz band include

- EIRP must be lower then 100 mW
- For crossing the public domain over a distance > 300m the user must have the authorization of the BIPT.
- No duplex working

36.2.9 Luxembourg Notification

For the 2.4 GHz band, point-to-point or point-to-multipoint operation is only allowed on campus areas. 5.4GHz products can only be used for mobile services.

36.2.10 Czech Republic Notification

2.4 GHz products can be operated in accordance with the Czech General License No. GL-12/R/2000.

5.4 GHz products can be operated in accordance with the Czech General License No. GL-30/R/2000.

36.2.11 Norway Notification

Use of the frequency bands 5725-5795 / 5815-5850 MHz are authorized with maximum radiated power of 4 W EIRP and maximum spectral power density of 200 mW/MHz. The radio equipment shall implement Dynamic Frequency Selection (DFS) as defined in Annex 1 of ITU-R Recommendation M.1652 / EN 301 893. Directional antennae with a gain up to 23 dBi may be used for fixed point-to-point links. The power flux density at the border between Norway and neighboring states shall not exceed – 122.5 dBW/m^2 measured with a reference bandwidth of 1 MHz.

Cyclone 5.7 GHz connectorized products have been notified for use in Norway and are compliant when configured to meet the above National requirements. Users shall ensure that DFS functionality is enabled, maximum EIRP respected for a 20 MHz channel, and that channel spacings comply with the allocated frequency band to protect Road Transport and Traffic Telematics services (for example, 5735, 5755, 5775 or 5835 MHz are suitable carrier frequencies). Note that for directional fixed links, TPC is not required, conducted transmit power shall not exceed 30 dBm, and antenna gain is restricted to 23 dBi (maximum of 40W from the Cyclone 5.7 GHz connectorized products).

36.2.12 Greece Notification

The outdoor use of 5470-5725MHz is under license of EETT but is being harmonized according to the CEPT Decision ECC/DEC/(04) 08, of 9th July. End users are advised to contact the EETT to determine the latest position and obtain any appropriate licenses.

36.2.13 Brazil Notification

Local regulations do not allow the use of 900 MHz, 2.4 GHz, or 5.2 GHz Cyclone modules in Brazil.

For compliant operation of an AP in the 5.7 GHz band, the Equivalent Isotropic Radiated Power from the built-in patch antenna and any associated reflector dish or LENS shall not exceed 36 dBm (4 W). When using the passive reflector (18 dB), transmitter output power must be configured no higher than 11 dBm. When using the LENS (10 dB at 5.7 GHz), transmitter output power must be configured no higher than 19 dBm.

For compliant operation in the 5.4 GHz band, the Equivalent Isotropic Radiated Power from the built-in patch antenna and any associated reflector dish or LENS shall not exceed 30 dBm (1 W). When using the passive reflector (18 dB), transmitter output power must be configured no higher than 5 dBm. When using the LENS (9 dB at 5.4 GHz), transmitter output power must be configured no higher than 14 dBm. When not using the passive reflector or the LENS, the transmitter output power of the radio must be configured no higher than 23 dBm.

The operator is responsible for enabling the DFS feature on any Cyclone 5.4 GHz radio by setting the Region Code to “Brazil”, including after the module is reset to factory defaults.

Important Note: This equipment operates as a secondary application, so it has no rights against harmful interference, even if generated by similar equipment, and cannot cause harmful interference on systems operating as primary applications.

36.2.14 Australia Notification

900 MHz modules must be set to transmit and receive only on center channels of 920, 922, or 923 MHz so as to stay within the ACMA approved band of 915 MHz to 928 MHz for the class license and not interfere with other approved users.

After taking into account antenna gain (in dBi), 900 MHz modules' transmitter output power (in dBm) must be set to stay within the legal regulatory limit of 30 dBm (1 W) EIRP for this 900 MHz frequency band.

36.2.15 Labeling and Disclosure Table for China

The People's Republic of China requires that Last Mile Gear'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▪联苯 (PBB)	多▪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 68: Disclosure Table

36.3 RF EXPOSURE

For important information on RF exposure and separation distances see Section 15.1, Exposure Separation Distances, on Page 169.

36.4 LEGAL NOTICES

36.4.1 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 LAST MILE GEAR, 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 Last Mile Gear agree as follows:

Grant of License. Subject to the following terms and conditions, Last Mile Gear, 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. Last Mile Gear (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 Last Mile Gear'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 Last Mile Gear'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 Last Mile Gear 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. Last Mile Gear warrants for a period of ninety (90) days from Last Mile Gear'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 Last Mile Gear's published specifications for that release level of the Software. The written materials are provided "AS IS" and without warranty of any kind. Last Mile Gear's entire liability and your sole and exclusive remedy for any breach of the foregoing limited warranty will be, at Last Mile Gear'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 LAST MILE GEAR, AND LAST MILE GEAR 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. LAST MILE GEAR 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 LAST MILE GEAR OR AN AGENT THEREOF SHALL CREATE A WARRANTY OR IN ANY WAY INCREASE THE SCOPE OF THIS WARRANTY. LAST MILE GEAR 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 LAST MILE GEAR 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 Last Mile Gear or a Last Mile Gear representative has been advised of the possibility of such damage. Last Mile Gear'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. Last Mile Gear shall not be responsible for maintenance or support of the software. By accepting the license granted under this agreement, you agree that Last Mile Gear 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 Last Mile Gear 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 Last Mile Gear equipment on which it operates; or 2) if you are a Last Mile Gear licensed distributor, when you are transferring the Software either together with such Last Mile Gear 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 Last Mile Gear 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. Last Mile Gear 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 Last Mile Gear 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 Last Mile Gear 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.

36.4.2 Hardware Warranty in U.S.

Last Mile Gear 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, Last Mile Gear 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.

36.4.3 Limit of Liability

IN NO EVENT SHALL LAST MILE GEAR 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 LAST MILE GEAR 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 LAST MILE GEAR'S LIABILITY EXCEED THE AMOUNT YOU PAID FOR THE PRODUCT.

37 ADDITIONAL RESOURCES

Cyclone provides two additional resources where you can raise questions and find answers:

- Cyclone Community Forums at http://Last Mile Gear.Cyclonewireless.com/support/community/.
  This resource facilitates communication with other users and with authorized Cyclone experts. Available forums include General Discussion, Network Monitoring Tools, and Suggestions.
- Cyclone Knowledge Base at http://Last Mile Gear.Cyclonewireless.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 Cyclone system.)
  - Product Alerts
  - Helpful Hints
  - FAQs (frequently asked questions)
  - Hardware Support
  - Software Support
  - Tools

38 HISTORY OF DOCUMENTATION

This section is a placeholder where changes for Issue 2 and later of this *Cyclone System Release 8 User Guide* will be listed.

GLOSSARY

~.	The command that terminates an SSH Secure Shell session to another server. Used on the Bandwidth and Authentication Manager (BAM) master server in the database replication setup.
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 Cyclone modules.
169.254.1.1	IP address default in Cyclone 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 Cyclone 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.
ACT/4	Second-from-left LED in the module. In the operating mode, this LED is lit when data activity is present on the Ethernet link. 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.
Activate	To provide feature capability to a module, but not to *enable* (turn on) the feature in the module. See also Enable.
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.

Advanced Encryption Standard	Over-the-air link option that provides extremely secure wireless connections. Advanced Encryption Standard (AES) uses 128-bit secret keys as directed by the government of the U.S.A. AES is not exportable and requires a special AP to process the large keys.
AES	See Advanced Encryption Standard.
Aggregate Throughput	The sum of the throughputs in the uplink and the downlink.
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.
Apache	A trademark of Apache Software Foundation, used with permission.
APAS	Access Point Authentication Server. Licensed to authenticate SMs that attempt to register to it. The AP licensed as APAS may or may not have authentication *enabled* (turned on). See also Activate and Enable.
API	Application programming interface for web services that supports Prizm integration with an operations support systems (OSS) such as a customer relationship management (CRM), billing, or provisioning system.
APs MIB	Management Information Base file that defines objects that are specific to the Access Point Module or Backhaul timing master. See also Management Information Base.
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.
ASN.1	Abstract Syntax Notation One language. The format of the text files that compose the Management Information Base.
Attenuation	Reduction of signal strength caused by the travel from the transmitter to the receiver, and caused by any object between. In the absence of objects between, a signal that has a short wavelength experiences a high degree of attenuation nevertheless.
Authentication Key	Software key that correlates to the random number that the Bandwidth and Authentication Manager (BAM) server generates and sends in a challenge through the AP to the SM. The network operator can create and, at some security risk, send this key over the air to the SM. The SQL database in the BAM server correlates this key to QoS information about the SM. The format of this key is 32 hexadecimal characters of 0 to 9 and a to f, padded with leading zeroes in Release 4.2.3 and later. This key must be unique to the individual SM.

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.
BAM	Bandwidth and Authentication Manager. A Cyclone software product that operates on a Linux server to manage bandwidth, high-priority channel, and VLAN settings individually for each registered Subscriber Module. This software also provides secure Subscriber Module authentication and user-specified encryption keys. The upgrade path for this product is to Prizm Release 2.0 or later.
BER	Bit Error Rate. The ratio of incorrect data received to correct data received.
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.
Bit Error Rate	Ratio of incorrect data received to correct data received.
Box MIB	Management Information Base file that defines module-level objects. See also Management Information Base.
BRAID	Stream cipher that the TIA (Telecommunications Industry Association) has standardized. The secret keys in both modules communicate with each other to establish the Data Encryption Standard key. See Data Encryption Standard.
Bridge	Network element that uses the physical address (not the logical address) of another to pass data. The bridge passes the data to either the destination address, if found in the simple routing table, or to all network segments other than the one that transmitted the data. Cyclone modules are Layer 2 bridges except that, where NAT is enabled for an SM, the SM is a Layer 3 switch. Compare to Switch and Router, and see also NAT.
Bridge Entry Timeout Field	Value that the operator sets as the maximum interval for no activity with another module, whose MAC address is the Bridge Entry. This interval should be longer than the ARP (Address Resolution Protocol) cache timeout of the router that feeds the network.
Buckets	Theoretical data repositories that can be filled at preset rates or emptied when preset conditions are experienced, such as when data is transferred.

Burst	Preset amount limit of data that may be continuously transferred.
C/I Ratio	Ratio of intended signal (carrier) to unintended signal (interference).
Cyclone	A trademark of Last Mile Gear, Inc.
Cyclone.xml	File that stores specifications for the Bandwidth and Authentication Manager (BAM) GUI.
Carrier-to-interference Ratio	Ratio of intended reception to unintended reception.
CarSenseLost Field	This field displays how many carrier sense lost errors occurred on the Ethernet controller.
CAT 5 Cable	Cable that delivers Ethernet communications from module to module. Later modules auto-sense whether this cable is wired in a straight-through or crossover scheme.
cdf	Cyclone Data Formatter tool that creates an initial ESN Data Table. Inputs for this tool include a list of SM ESNs and default values of sustained data rates and burst allocations for each listed ESN.
chkconfig	A command that the Linux® operating system accepts to enable MySQL® and Apache™ Server software for various run levels of the mysqld and httpd utilities.
CIR	See Committed Information Rate.
Cluster Management Module	Module that provides power, GPS timing, and networking connections for an AP cluster. Also known as CMM. If this CMM is connected to a Backhaul Module, then this CMM is the central point of connectivity for the entire site.
CMM	Cluster Management Module. A module that provides power, GPS timing, and networking connections for an Access Point cluster. If this CMM is connected to a Backhaul Module (BH), then this CMM is the central point of connectivity for the entire site.
CodePoint	See DiffServ.
Color Code Field	Module parameter that identifies the other modules with which communication is allowed. The range of values is 0 to 255. When set at 0, the Color Code does not restrict communications with any other module.
Committed Information Rate	For an SM or specified group of SMs, a level of bandwidth that can be guaranteed to never fall below a specified minimum. In the Cyclone implementation, this is controlled by the Low Priority Uplink CIR, Low Priority Downlink CIR, High Priority Uplink CIR, and High Priority Downlink CIR parameters.

Community String Field	Control string that allows a network management station to access MIB information about the module.
CPE	Customer premises equipment.
CRCError Field	This field displays how many CRC errors occurred on the Ethernet controller.
CRM	Customer relationship management system.
Data Encryption Standard	Over-the-air link option that uses secret 56-bit keys and 8 parity bits. Data Encryption Standard (DES) performs a series of bit permutations, substitutions, and recombination operations on blocks of data.
Date of Last Transaction	A field in the data that the `cmd show esn` command generates from data in the SQL database in the Bandwidth and Authentication Manager (BAM) server. This field identifies the date of the most recent authentication attempt by the SM. Expressed in the database output as DLT.
Dell	A trademark of Dell, Inc.
Demilitarized Zone	Internet Protocol area outside of a firewall. Defined in RFC 2647. See http://www.faqs.org/rfcs/rfc2647.html.
DES	Data Encryption Standard. An over-the-air link option that uses secret 56-bit keys and 8 parity bits. DES performs a series of bit permutations, substitutions, and recombination operations on blocks of data.
Desensed	Received an undesired signal that was strong enough to make the module insensitive to the desired signal.
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 the Cyclone system. See http://www.faqs.org/rfcs/rfc2131.html. See also Static IP Address Assignment.
Diffraction	Partial obstruction of a signal. Typically diffraction attenuates a signal so much that the link is unacceptable. However, in some instances where the obstruction is very close to the receiver, the link may be acceptable.

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. Cyclone 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.
DLT	Date of last transaction. A field in the data that the `cmd show esn` command generates from data in the SQL database in the Bandwidth and Authentication Manager (BAM) server. This field identifies the date of the most recent authentication attempt by the SM.
DMZ	Demilitarized Zone as defined in RFC 2647. An Internet Protocol area outside of a firewall. See http://www.faqs.org/rfcs/rfc2647.html.
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 Cyclone 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.
Element Pack	A license for Prizm management of a multi-point sector and covers the AP and up to 200 SMs, a backhaul link, or an Powerline LV link.
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.
Engine	Bandwidth and Authentication Manager (BAM) interface to the AP and SMs. Unique sets of commands are available on this interface to manage parameters and user access. Distinguished from SSE. See also SSE.
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.

ESN Data Table	Table in which each row identifies data about a single SM. In tab-separated fields, each row stores the ESN, authentication key, and QoS information that apply to the SM. The operator can create and modify this table. This table is both an input to and an output from the Bandwidth and Authentication Manager (BAM) SQL database, and should be identically input to redundant BAM servers.
/etc/services	File that stores telnet ports on the Bandwidth and Authentication Manager (BAM) server.
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.
Fade Margin	The difference between strength of the received signal and the strength that the receiver requires for maintaining a reliable link. A higher fade margin is characteristic of a more reliable link. Standard operating margin.
FCC	Federal Communications Commission of the U.S.A.
Feature Activation Key	Software key file whose file name includes the ESN of the target Cyclone 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.
Frame Spreading	Transmission of a beacon in only frames where the receiver expects a beacon (rather than in every frame). This avoids interference from transmissions that are not intended for the receiver.
Frame Timing Pulse Gated Field	Toggle parameter that prevents or allows the module to continue to propagate GPS sync timing when the module no longer receives the timing.
Free Space Path Loss	Signal attenuation that is naturally caused by atmospheric conditions and by the distance between the antenna and the receiver.
Fresnel Zone	Space in which no object should exist that can attenuate, diffract, or reflect a transmitted signal before the signal reaches the target receiver.

FSK	Frequency Shift Keying, a variation of frequency modulation to transmit data, in which two or more frequencies are used.
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.
indiscards count Field	How many inbound packets were discarded without errors that would have prevented their delivery to a higher-layer protocol. (Some of these packets may have been discarded to increase buffer space.)
inerrors count Field	How many inbound packets contained errors that prevented their delivery to a higher-layer protocol.
innucastpkts count Field	How many inbound non-unicast (subnetwork-broadcast or subnetwork-multicast) packets were delivered to a higher-layer protocol.

inoctets count Field	How many octets were received on the interface, including those that deliver framing information.
Intel	A registered trademark of Intel Corporation.
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.
Jitter	Timing-based measure of the reception quality of a link. An acceptable link displays a jitter value between 0 and 4 for a 10-Mbps Backhaul timing slave in Release 4.0 and later, between 0 and 9 for a 20-Mbps Backhaul timing slave, or between 5 and 9 for any Subscriber Module or for a Backhaul timing slave in any earlier release.
L2TP over IPSec	Level 2 Tunneling Protocol over IP Security. One of several virtual private network (VPN) implementation schemes. Regardless of whether Subscriber Modules have the Network Address Translation feature (NAT) enabled, they support VPNs that are based on this protocol.
Late Collision Field	This field displays how many late collisions occurred on the Ethernet controller. A normal collision occurs during the first 512 bits of the frame transmission. A collision that occurs after the first 512 bits is considered a late collision. A late collision is a serious network problem because the frame being transmitted is discarded. A late collision is most commonly caused by a mismatch between duplex configurations at the ends of a link segment.
Latency Tolerance	Acceptable tolerance for delay in the transfer of data to and from a module.
Line of Sight	Wireless path (not simply visual path) direct from module to module. The path that results provides both ideal aim and an ideal Fresnel zone.
Linux	A registered trademark of Linus Torvalds.

LNK/5	Furthest left LED in the module. In the operating mode, this LED is continuously lit when the Ethernet link is present. 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.
Logical Unit ID	Final octet of the 4-octet IP address of the module.
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.
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).
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.
Maximum Information Rate	The cap applied to the bandwidth of an SM or specified group of SMs. In the Cyclone implementation this is controlled by the Sustained Uplink Data Rate, Uplink Burst Allocation, Sustained Downlink Data Rate, and Downlink Burst Allocation parameters.
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).
MIR	See Maximum Information Rate.
MySQL	A registered trademark of MySQL AB Company in the United States, the European Union, and other countries.
mysqladmin	A command to set the administrator and associated password on the Bandwidth and Authentication Manager (BAM) server.

mysql-server	Package group that enables the SQL Database Server application in the Red Hat® Linux® 9 operating system to provide SQL data for Bandwidth and Authentication Manager (BAM) operations.
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.
Object	Network variable that is defined in the Management Information Base.
OptiPlex	A trademark of Dell, Inc.
OSS	Operations support system, such as a customer relationship management (CRM), billing, or provisioning system. The application programming interface (API) for Prizm supports integrating Prizm with an OSS.

outdiscards count Field	How many outbound packets were discarded without errors that would have prevented their transmission. (Some of these packets may have been discarded to increase buffer space.)
outerrrors count Field	How many outbound packets contained errors that prevented their transmission.
outnucastpkts count Field	How many packets for which the higher-level protocols requested transmission to a non-unicast (subnetwork-broadcast or subnetwork-multicast) address. The number includes those that were discarded or not sent.
outoctets count Field	How many octets were transmitted out of the interface, including those that deliver framing information.
outucastpkts count Field	How many packets for which the higher-level protocols requested transmission to a subnetwork-unicast address. The number includes those that were discarded or not sent.
Override Plug	Device that enables the operator to regain control of a module that has been locked by the No Remote Access feature, the 802.3 Link Disable feature, or a password or IP address that cannot be recalled. This device can be either fabricated on site or ordered.
Pentium	A registered trademark of Intel Corporation.
php-mysql	Package group that enables the Web Server application in the Red Hat® Linux® 9 operating system to provide data from the SQL Database Server application as PHP in the Bandwidth and Authentication Manager (BAM) 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.
Power Control	Feature in Release 4.1 and later that allows the module to operate at less than 18 dB less than full power to reduce self-interference.
PPTP	Point to Point Tunneling Protocol. One of several virtual private network implementations. With the Network Address Translation (NAT) feature enabled, Subscriber Modules *do not* support VPNs that are based on this protocol. With NAT disabled, they do support VPNs that are based on this protocol.
Prizm	The Cyclone software product that allows users to partition their entire Cyclone 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 Cyclone 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.
Quick Start	Interface page that requires minimal configuration for initial module operation.
Radio Signal Strength Indicator	Relative measure of the strength of a received signal. An acceptable link displays an Radio Signal Strength Indicator (RSSI) value of greater than 700.
Random Number	Number that the Bandwidth and Authentication Manager (BAM) generates, invisible to both the SM and the network operator, to send to the SM as a challenge against an authentication attempt.
Reader	A registered trademark of Adobe Systems, Incorporated.
Recharging	Resumed accumulation of data in available data space (buckets). See Buckets.
Red Hat	A registered trademark of Red Hat, Inc.

Reflection Change of direction and reduction of amplitude of a signal that encounters an object larger than the wavelength. Reflection may cause an additional copy of the wavelength to arrive at after the original, unobstructed wavelength arrives. This causes partial cancellation of the signal and may render the link unacceptable. However, in some instances where the direct signal cannot be received, the reflected copy may be received and render an otherwise unacceptable link acceptable.

Registrations MIB Management Information Base file that defines registrations for global items such as product identities and product components. See also Management Information Base.

repl-m A command that sets up the database replication process on a Bandwidth and Authentication Manager (BAM) master server, uses SFTP to copy both the database and the `repl-s` script to a BAM slave server, and remotely executes the `repl-s` script on the BAM slave server. See Master, Slave, `repl-s`, Secure Shell, and SFTP.

repl-s A command that sets up the database replication process on a Bandwidth and Authentication Manager (BAM) slave server. See Master, Slave, and `repl-m`.

RES Result. A field in the data that the `cmd show esn` command generates from the SQL database in the Bandwidth and Authentication Manager (BAM) server.

RetransLimitExp Field This field displays how many times the retransmit limit has expired.

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 Cyclone 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.

RPM Red Hat® Package Manager.

rpm A command that the Linux® operating system accepts to identify the version of Linux® software that operates on the Bandwidth and Authentication Manager (BAM) server.

RSSI Radio Signal Strength Indicator. A relative measure of the strength of a received signal. An acceptable link displays an RSSI value of greater than 700.

RxBabErr Field	This field displays how many receiver babble errors occurred.
RxOverrun Field	This field displays how many receiver overrun errors occurred on the Ethernet controller.
SDK	*PrizmEMS™ Software Development Kit (SDK)*—the document that provides server administrator tasks, GUI developer information for console automation that allows higher-level systems to launch and appropriately display the Prizm management console. The SDK also describes the how to define new element types and customize the Details views.
Secure Shell	A trademark of SSH Communications Security.
Self-interference	Interference with a module from another module in the same network.
SES/2	Third-from-right LED in the module. In the Access Point Module and Backhaul timing master, this LED is unused. 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.
Session Key	Software key that the SM and Bandwidth and Authentication Manager (BAM) separately calculate based on that both the authentication key (or the factory-set default key) and the random number. BAM sends the session key to the AP. Neither the subscriber nor the network operator can view this key. See also Random Number.
SFTP	Secure File Transfer Protocol.
Simple Network Management Protocol	Standard that is used for communications between a program (agent) in the network and a network management station (monitor). Defined in RFC 1157. See http://www.faqs.org/rfcs/rfc1157.html.
skey	Software key that correlates to the random number that the Bandwidth and Authentication Manager (BAM) server generates and sends in a challenge through the AP to the SM. The network operator can create and, at some security risk, send this key over the air to the SM. The SQL database in the BAM server correlates this key to QoS information about the SM. The format of this key is 32 hexadecimal characters of 0 to 9 and a to f. This key must be unique to the individual SM. Also known as authentication key.
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.
SM MIB	Management Information Base file that defines objects that are specific to the Subscriber Module or Backhaul timing slave. See also Management Information Base.
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.
SOAP	Simple Object Access Protocol (SOAP). The protocol that the Northbound Interface in Prizm uses to support integration of Prizm with an operations support systems (OSS) such as a customer relationship management (CRM), billing, or provisioning system
SSE	Bandwidth and Authentication Manager (BAM) interface to the SQL server. Unique sets of commands are available on this interface to manage the BAM SQL database and user access. Distinguished from Engine. See also Engine.
Standard Operating Margin	See Fade Margin.
Static IP Address Assignment	Assignment of Internet Protocol address that can be changed only manually. Thus static IP address assignment requires more configuration time and consumes more of the available IP addresses than DHCP address assignment does. RFC 2050 provides guidelines for the static allocation of IP addresses. See http://www.faqs.org/rfcs/rfc2050.html. See also DHCP.
su -	A command that opens a Linux® operating system session for the user `root`.
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.
Sustained Data Rate	Preset rate limit of data transfer.

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.
SYN/1	Second-from-right LED in the module. In the Access Point Module or Backhaul timing master, as in a registered Subscriber Module or Backhaul timing slave, this LED is continuously lit to indicate the presence of sync. In the operating mode for a Subscriber Module or Backhaul timing slave, this LED flashes on and 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.
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 Cyclone system uses Port 3306:tcp for MySQL® database communications, Port 9080:tcp for SSE `telnet` communications, and Port 9090:tcp for Engine `telnet` communications.
TDD	Time Division Duplexing.
TDMA	Time Division Multiple Access.
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 Cyclone system-specific textual conventions. See also Management Information Base.
Time of Last Transaction	A field in the data that the `cmd show esn` command generates from data in the SQL database in the Bandwidth and Authentication Manager (BAM) server. This field identifies the time of day of the most recent authentication attempt by the SM. Expressed in the database output as TLT.
TLT	Time of last transaction. A field in the data that the `cmd show esn` command generates from data in the SQL database in the Bandwidth and Authentication Manager (BAM) server. This field identifies the time of day of the most recent authentication attempt by the SM.

TNAF	Total number of authentication requests failed. A field in the data that the `cmd show esn` command generates from the SQL database in the Bandwidth and Authentication Manager (BAM) server. This field indicates how many times the SM (identified by ESN in the related data) attempted to authenticate but was denied by BAM.
TNAR	Total number of authentication requests. A field in the data that the `cmd show esn` command generates from the SQL database in the Bandwidth and Authentication Manager (BAM) server. This field indicates how many times the SM (identified by ESN in the related data) attempted to authenticate, regardless of whether the attempt succeeded.
Tokens	Theoretical amounts of data. See also Buckets.
TOS	8-bit field in that prioritizes data in a IP transmission. See http://www.faqs.org/rfcs/rfc1349.html.
TxUnderrun Field	This field displays how many transmission-underrun errors occurred on the Ethernet controller.
UDP	User Datagram Protocol. A set of Network, Transport, and Session Layer protocols that RFC 768 defines. These protocols include checksum and address information but does not retransmit data or process any errors. See http://www.faqs.org/rfcs/rfc768.html.
udp	User-defined type of port.
U-NII	Unlicensed National Information Infrastructure radio frequency band, in the 5.1-GHz through 5.8-GHz ranges.
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 on Cyclone System Release 4.2 or later 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.