



Diagnostics and Troubleshooting

This chapter describes the diagnostic pages in the management system and provides troubleshooting procedures for basic problems with the access point. For the most up-to-date, detailed troubleshooting information, refer to the Cisco TAC website at <http://www.cisco.com/tac> Select **Wireless LAN** under Top Issues.

Sections in this chapter include:

- [Using Diagnostic Pages, page 13-2](#)
- [Using Command-Line Diagnostics, page 13-15](#)
- [Tracing Packets, page 13-24](#)
- [Checking the Top Panel Indicators, page 13-28](#)
- [Checking Basic Settings, page 13-30](#)
- [Resetting to the Default Configuration, page 13-32](#)

Using Diagnostic Pages

The management system contains three diagnostic pages that provide detailed statistics and event records for the access point:

- The [Network Diagnostics Page](#) provides access to radio diagnostic tests and provides links to the VLAN Summary Status and SSID statistics pages for access point radios.
- The [Network Ports Page](#) lists statistics on data transmitted and received by the access point.
- The [Event Log Page](#) lists network events.

Each page is described in the sections below.

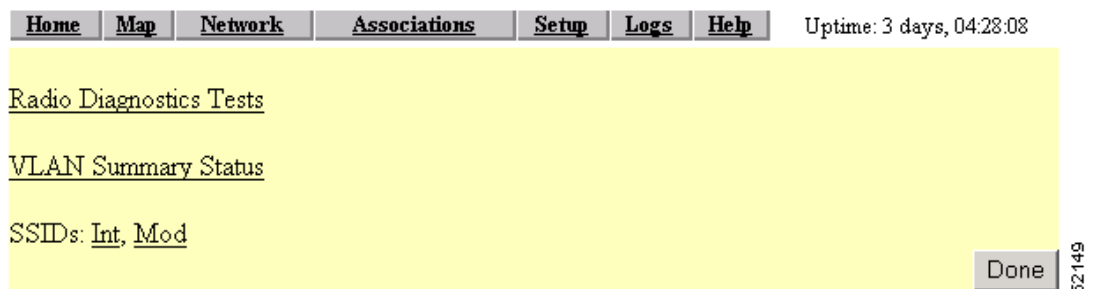
Network Diagnostics Page

Use the Network Diagnostics page to access the following diagnostic pages:

- Radio diagnostics tests
- VLAN Summary Status page
- SSID pages for the internal or module radio

[Figure 13-1](#) shows the Network Diagnostics page.

Figure 13-1 Network Diagnostics Page



Follow this link path to reach the Network Diagnostics page:

1. On the Summary Status page or Setup page, click **Diagnostics** in the Network Ports row.

Selections on the Network Diagnostics Page

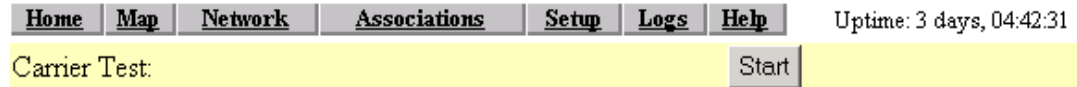
The Network Diagnostics page contains the following selections:

- Radio Diagnostics Tests
- VLAN Summary Status
- SSIDs: Int, Mod

Radio Diagnostics Tests

Click **Radio Diagnostics Tests** to access the Radio Diagnostics page and conduct a carrier test ([Figure 13-2](#)).

Figure 13-2 Radio Diagnostics Page



The carrier test helps you determine which radio frequencies contain the most radio activity and noise that could interfere with radio signals to and from the access point.

Use the carrier test to determine the best frequency for the access point to use. When you conduct a carrier test, make sure all wireless networking devices within range of the access point are operating to make the test results reflect a realistic radio environment.

When you click **Start**, the radio scans the access point's available frequencies and displays the radio activity in the Carrier Test window.

**Note**

The access point drops all associations with wireless networking devices during the carrier test.

Carrier Test

The carrier test measures the amount of radio activity on each frequency available to the access point. Use the carrier test to determine the best frequency for the access point to use. When you conduct a carrier test, make sure all wireless networking devices within range of the access point are operating to make the test results reflect a realistic radio environment.

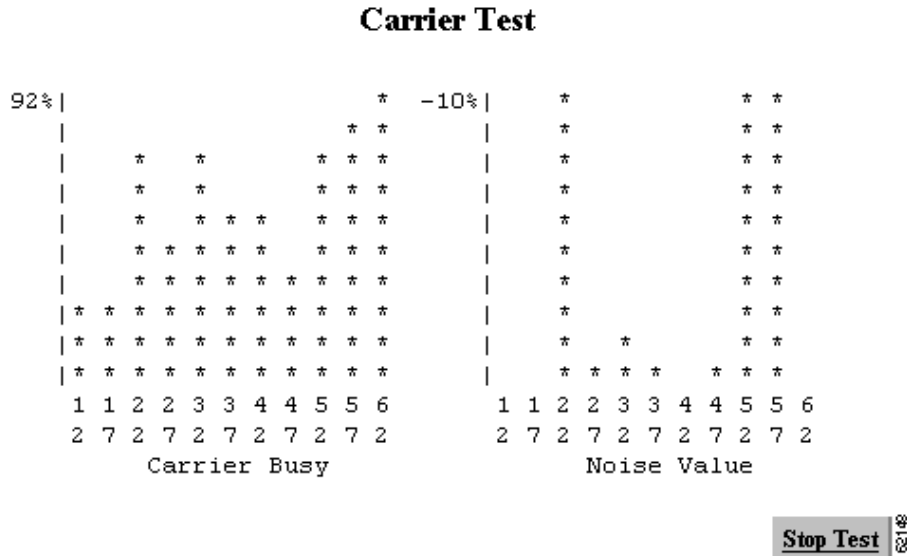
When you click **Start**, the radio scans the access point's available frequencies and displays the radio activity in the Carrier Test window.

**Note**

The access point drops all associations with wireless networking devices during the carrier test.

Figure 13-3 shows an example Carrier Test window.

Figure 13-3 Carrier Test Window



The bar graph on the left side of the window displays the percentage used for each frequency; the highest current percentage used is labeled on the top left of the graph. In this example, the highest percentage used for any frequency is 92. The access point's available frequencies are listed vertically across the bottom of the graph, from 2412 to 2462 GHz. The access point's channel 1 is 2412 GHz, channel 2 is 2417 GHz, and so on up to channel 11, which is 2462 GHz.

The bar graph on the right side of the window displays the amount of noise on each frequency. Noise is a measurement of the signal the radio receives when it is not receiving packets. Even in an environment in which the radio receives a great deal of noise, it might also receive a strong data signal. Click **Stop Test** in the window or on the Radio Diagnostics page to stop the test.

VLAN Summary Status

Click **VLAN Summary Status** to reach the VLAN Summary Status page for your access point. Figure 13-4 shows a typical VLAN Summary Status page.

Figure 13-4 VLAN Summary Status Page

ID	Name	Enabled?	Def. Pri.	Def. Pol. Grp.	MIC	TKIP	Key Rotate	Alert?	Encryption
1(N)	Native VLAN	yes	best effort	[0]	none	Cisco	0	no	full
2		no	best effort	[0]	none	none	0	no	optional
3	Part-Time	yes	best effort	[0]	none	Cisco	0	no	full
4	Guest	yes	best effort	[0]	none	none	0	no	optional
5	Maintenance	yes	best effort	[0]	none	none	0	no	full

Done

The following links are available on the page:

- VLAN Detailed Setup—takes you to the VLAN Setup page, from which you can add, remove, or edit your VLAN configuration.

- ID(#)—takes you to the VLAN Setup page for the VLAN ID selected where you can edit the configuration.
- Def. Pol. Grp (if set)—takes you to the Policy Groups page, where you can edit the configuration.

Service Sets

The Service Sets link takes you to the AP Radio Service Set Summary Status page for your access point. shows a typical SSID Summary Status page for the radio.

Figure 13-5 AP Radio Module Service Set Summary Status Page

Service Set Detailed Setup											
Idx	SSID	Curr. Assoc	Max Assoc	Auth Alg.	Def. Pol. Grp.	VLAN	Enabled?	MIC	TKIP	Key Rotate	Encryption
<u>0</u>	Bald Eagle 2	0	0	open	[0]			none	none	0	none

Done 88504

The following links are available on this page:

- Service Set Detailed Setup—takes you to the AP Radio Service Sets page, from which you can create, remove, or edit your SSID configuration.
- Idx(#)—takes you to the AP Radio Primary SSID page of the number selected where you can edit its configuration.

Network Ports Page

The Network Ports page contains a table listing information for the access point's Ethernet and radio ports. [Figure 13-6](#) shows a Network Ports page example.

Figure 13-6 Network Ports Page

Network Diagnostics			
Home	Map	Network	Associations
			Setup
			Logs
			Help
Uptime: 4 days, 23:27:31			
Name	Ethernet*	Root Radio	Bridge:BR350 West
Status	Up	Up	Up
Max. Mb/s	100.0	11.0	11.0
IP Addr.	10.84.137.71	10.84.137.71	10.84.137.71
MAC Addr.	00409631535e	00409631535e	00409631535e
Radio SSID		bridge	
Receive			
unicast pkts.	33477	1043	114
multicast pkts.	948580	0	589
total bytes	48992558	156555	131190
errors	0	0	0
discards	0	0	0
forwardable pkts.	132981	39171	130
filtered pkts.	0	1303	0
Transmit			
unicast pkts.	45653	1073	117
multicast pkts.	438983	213	773
total bytes	37949231	288969	93564
errors	0	18	0
discards	0	0	0
forwarded pkts.	524980	51601	240

Click the **Network** link at the top of any main management system page to reach the Network Ports page, or click **Network Ports** on the Summary Status home page.

The following links are available on this page:

- Network Diagnostics link—displays the Cisco Network Diagnostics page, where you can select diagnostic tests.
- VLAN—displays the VLAN Summary Status page, where you can view the configuration of existing VLANs. A VLAN Detailed Setup link on this page leads to the VLAN Setup page, where you can create a new VLAN, edit, or remove an existing VLAN.
- Service Sets—displays the Service Set Summary Status page, where you can view the configuration of existing SSIDs. A Service Set Detailed Setup page leads to the Internal Service Sets page, where you can add a new SSID, edit, or remove an existing SSID.

The Network Ports table is divided into three sections: identifying information and status, data received, and data transmitted. Each row in the table is described below.

Identifying Information and Status

- Name—Displays the name of the network interface port. An asterisk (*) next to the name identifies the port as the primary port for the access point.

The port names are links to a detailed page for each port. See the “[Ethernet Port Page](#)” section on page 13-7 for information on the Ethernet Port page and the “[AP Radio Page](#)” section on page 13-10 for information on the AP Radio Port page.

- Status—Displays one of three possible operating states for the port:

- Up—The port is operating properly.
- Down—The port is not operating.
- Error—The port is operating but is in an error condition.
- Max. Mb/s—The maximum rate of data transmission in megabits per second.
- IP Addr.—The IP address for the port. When the access point is set up in standby mode the Ethernet and radio ports use different IP addresses. Use the AP Radio Identification page to assign an IP address to the radio port that is different from the Ethernet IP address. See the [“Settings on the AP Radio Identification Page” section on page 3-7](#) for details on the AP Radio Identification page.
- MAC (Media Access Control) Addr.—The Media Access Control (MAC) address is a unique identifier assigned to the network interface by the manufacturer.
- Radio SSID—A unique identifier that client devices use to associate with the access point. The SSID helps client devices distinguish between multiple wireless networks in the same vicinity.

Data Received

- Unicast pkts.—The number of packets received in point-to-point communication.
- Multicast pkts.—The number of packets received that were sent as a transmission to a set of nodes.
- Total bytes—The total number of bytes received.
- Errors—The number of packets determined to be in error.
- Discards—The number of packets discarded by the access point due to errors or network congestion.
- Forwardable pkts.—The number of packets received by the port that was acceptable or passable through the filters.
- Filtered pkts.—The number of packets that were stopped or screened by the filters set up on the port.

Data Transmitted

- Unicast pkts.—The number of packets transmitted in point-to-point communication.
- Multicast pkts.—The number of packets transmitted that were sent as a transmission to a set of nodes.
- Total bytes—Total number of bytes transmitted from the port.
- Errors—The number of packets determined to be in error.
- Discards—The number of packets discarded by the access point due to errors or network congestion.
- Forwarded pkts.—The number of packets transmitted by the port that was acceptable or passable through the filters.

Ethernet Port Page

When you click **Ethernet** in the Network Ports table, the browser displays the Ethernet Port page. This page lists detailed statistics on the access point’s Ethernet port. [Figure 13-7](#) shows an Ethernet Port page example.

Figure 13-7 Ethernet Port Page

Configuration		Set Properties	
Status of "fec0"	Up (primary)	Maximum Rate (Mb/s)	10.0
IP Address	172.16.24.0	MAC Address	00409625854d
Duplex	Full		
Statistics			
Receive		Transmit	
Unicast Packets	4620	Unicast Packets	3910
Multicast Packets	98350	Multicast Packets	1193
Total Bytes	13987582	Total Bytes	1238105
Total Errors	0	Total Errors	0
Discarded Packets	0	Discarded Packets	0
Forwardable Packets	105199	Forwarded Packets	3379
Filtered Packets	0		
Packet CRC Errors	0	Max Retry Packets	0
Carrier Sense Lost	0	Total Collisions	0
Late Collisions	0	Late Collisions	0
Overrun Packets	0	Underrun Packets	0
Packets Too Long	0		
Packets Too Short	0		
Packets Truncated	0		

49/11

Like the Network Ports page, the Ethernet Port page lists statistics in a table divided into sections. Each row in the table is explained in the following sections.

Configuration Information

- The top row of the Configuration section of the table contains a Set Properties link that leads to the Ethernet Hardware page.
- Status of “fec0”— “Fast Ethernet Controller” is part of Motorola's naming convention for the Ethernet device used by the access point. This field displays one of the three possible operating states for the port. The added term “primary” identifies the port as the primary port for the access point. Operating states include:
 - Up—The port is operating properly.
 - Down—The port is not operating.
 - Error—The port is in an error condition.
- Maximum Rate (Mb/s)—Maximum rate of data transmission in megabits per second.
- IP Address—The IP address of the port.
- MAC Address—The unique identifier assigned to the access point by the manufacturer.
- Duplex—The port's duplex setting, either half or full.

Receive Statistics

- Unicast Packets—The number of packets received in point-to-point communication.
- Multicast Packets—The number of packets received that were sent as a transmission to a set of nodes.
- Total Bytes—Total number of bytes received.
- Total Errors—Total number of packets determined to be in error.
- Discarded Packets—Packets discarded due to errors or network congestion.
- Forwardable Packets—Packets received by the port that were acceptable or passable through the filters.
- Filtered Packets—Packets that were stopped or screened by the filters set up on the port.
- Packet CRC Errors—Cyclic redundancy check (CRC) errors that were detected in a received packet.
- Carrier Sense Lost—The number of disconnects from the Ethernet network. Carrier sense lost events are usually caused by disconnected wiring.
- Late Collisions—Packet errors that probably were caused by over-long wiring problems. Late collisions could also indicate a failing NIC card.
- Overrun Packets—Ethernet packets that were discarded because the access point had a temporary overload of packets to handle.
- Packets Too Long—Ethernet packets that were larger than the maximum packet size of 1518 bytes.
- Packets Too Short—Ethernet packets that were shorter than the minimum packet size of 64 bytes.
- Packets Truncated—Corrupt or incomplete packets.

Transmit Statistics

- Unicast Packets—The number of packets transmitted in point-to-point communication.
- Multicast Packets—The number of packets transmitted that were sent as a transmission to a set of nodes.
- Total Bytes—Total number of bytes transmitted from the port.

- Total Errors—The number of packets determined to be in error.
- Discarded Packets—The number of packets discarded by the access point due to errors or network congestion.
- Forwarded Packets—The number of packets transmitted by the port that were acceptable or passable through the filters.
- Max Retry Packets—Packets which failed after being retried several times.
- Total Collisions—The number of packet collisions that occurred through this port.
- Late Collisions—Packet errors that were likely caused by overlong wiring problems. Could also indicate a failing NIC card.
- Underrun Packets—Packets failed to be sent because the access point was unable to keep up with the Ethernet controller.

AP Radio Page

When you click **AP Radio** in the Network Ports table, the browser displays the AP Radio Port page. This page lists detailed statistics on the access point's radio. [Figure 13-8](#) shows an AP Radio Port page example.

Figure 13-8 AP Radio Port Page

Home		Map		Network		Associations		Setup		Logs		Help		Uptime: 3 days, 16:21:20	
Options: Detailed Config. <input type="checkbox"/> Detailed Stats. <input type="checkbox"/> Individual Rates <input type="checkbox"/>														Apply	
Configuration														Set Properties	
Status of "awc0"	Up			Maximum Rate (Mb/s)	11.0										
IP Address	10.0.0.1			MAC Address	00059a38421d										
SSID	Test AP 2														
Operational Rates (Mb/s)	1.0B, 2.0B, 5.5B, 11.0B			Transmit Power (mW)	100										
Statistics														Refresh	
Receive				<i>Alert</i> <input type="checkbox"/>		Transmit				<i>Alert</i> <input type="checkbox"/>					
Unicast Packets	33300			Unicast Packets	15555										
Multicast Packets	0			Multicast Packets	31351										
Total Bytes	3431551			Total Bytes	16870368										
Total Errors	1			Total Errors	2										
Discarded Packets	1			Discarded Packets	0										
Forwardable Packets	25088			by CoS (0-7): 0, 0, 0, 0, 0, 0, 0, 0											
Filtered Packets	0			Forwarded Packets	70582										
Packet CRC Errors	51119453			Max Retry Packets	2										
Packet WEP Errors	0			Total Retries	4541										
Overrun Packets	0			Cancelled Assoc. Lost	0										
Duplicate Packets	1236			Cancelled AID	10										
Lifetime Exceeded	0			Lifetime Exceeded	0										
MIC Packets	0			MIC Packets	0										
MIC Errors	0			MIC Errors	0										
MIC Sequ. Errors	0														
MIC Auth. Errors	0														

49696

Like the Network Ports and Ethernet Port pages, the AP Radio Port page lists statistics in a table divided into sections. Each row in the table is explained below.

Configuration Information

- The top row of the Configuration section of the table contains a Set Properties link that leads to the AP Radio Hardware page. See the “[Entering Radio Hardware Information](#)” section on page 3-9 for details on the AP Radio Hardware page.
- Status of “awc0”—*awc0* (Aironet Wireless Communications) is part of Cisco Aironet's naming convention for this radio. This field displays one of three possible operating states:
 - Up—The port is operating properly.
 - Down—The port is not operating.
 - Error—The port is in an error condition.
- Maximum Rate (Mbps)—Maximum rate of data transmission in megabits per second. Data rates set to basic are followed by B.
- IP Addr.—The IP address of the radio port.
- MAC (Media Access Control) Addr.—A unique identifier assigned to the network interface by the manufacturer.
- SSID—The unique identifier that client devices use to associate with the access point radio. The SSID helps client devices distinguish between multiple wireless networks in the same vicinity.
- Operational Rates—The data transmission rates supported and enabled by the access point for communication with client devices.
- Transmit Power (mW)—The power level of radio transmission. You can reduce the transmit power to conserve power or reduce interference. Click **Set Properties** to display the AP Radio Hardware page, where you can change this setting.

Receive Statistics

- Unicast Packets—The number of packets received in point-to-point communication.
- Multicast Packets—The number of packets received that were sent as a transmission to a set of nodes.
- Total Bytes—The total number of bytes received.
- Total Errors—The total number of packets determined to be in error.
- Discarded Packets—Packets discarded due to errors or network congestion.
- Forwardable Packets—Packets received by the port that were acceptable or passable through the filters.
- Filtered Packets—Packets that were stopped or screened by the filters set up on the port.
- Packet CRC Errors—Cyclic redundancy check (CRC) errors that were detected in a received packet.
- Packet WEP Errors—Encryption errors received through this port.
- Overrun Packets—Packets that were discarded because the access point had a temporary overload of packets to handle.
- Duplicate Packets—Packets that were received twice because an acknowledgment was lost and the sender retransmitted the packet.

- Lifetime Exceeded—Fragmented packets that were dropped because it took too long to get the next fragment.
- MIC Packets—Total number of packets received since system startup and for which a MIC has been requested to be validated with the MMH algorithm.
- MIC Errors—Total number of packets received since system startup that failed MIC validation with the MMH algorithm.
- MIC Sequ. Errors—Total number of packets received since system startup that failed MIC validation with the MMH algorithm specifically due to sequence number and duplicate packet errors.
- MIC Auth. Errors—Total number of packets received since system startup that failed MIC validation with the MMH algorithm specifically due to cryptographic key-mismatch errors.

Transmit Statistics

- Unicast Packets—The number of packets transmitted in point-to-point communication.
- Multicast Packets—The number of packets transmitted that were sent as a transmission to a set of nodes.
- Total Bytes—The number of bytes transmitted from the port.
- Total Errors—The number of packets determined to be in error.
- Discarded Packets—The number of packets discarded by the access point due to errors or network congestion.
- Forwarded Packets—The number of packets transmitted by the port that were acceptable or passable through the filters.
- Max Retry Packets—The number of times request to send (RTS) reached the maximum retry number. Click **Set Properties** to display the AP Radio Hardware page, where you can set the maximum RTS value.
- Total Retries—The total number of retries that occurred through the radio port.
- Canceled Assoc. Lost—Packets dropped because a client device lost association with the access point.
- Canceled AID—Packets dropped by a repeater because it roamed to a different parent during a retransmission attempt.
- Lifetime Exceeded—Fragmented packets that were dropped because it took too long to deliver a fragment.
- MIC Packets—Total number of packets since system startup for which the access point has requested MIC to be calculated with the MMH algorithm before being submitted for transmission.
- MIC Errors—Total number of packets which have failed MIC calculation with the MMH algorithm before being submitted for transmission over this radio since system startup.
- MIC Sequ. Errors—Packets appear to have arrived either very late or out of sequence. This could be caused by a poor radio link or a replay.
- MIC Auth. Errors—The MIC signature is bad due to a calculation with the wrong cryptographic key. These errors could be caused by a simple misconfiguration of a WEP key, or by an attack.

Display Options

Figure 13-8 shows the basic AP Radio Port page. Three display options provide more details on the port configuration and operating statistics. The basic page provides all the information needed to monitor and administer the port in normal operation. You might need the other display options in comprehensive site surveys or advanced system troubleshooting. To select a display option, click an option checkbox and click **Apply**.

The display options include:

- Detailed Config.—Details on the radio port configuration, including request to send (RTS) and data retry settings, firmware and bootblock version levels, and regulatory domain code.
- Detailed Stats.—Twenty additional statistical fields covering packet fragments, collisions, and other errors.
- Individual Rates—Data transmission statistics for each data rate (1, 2, 5, and 11 Mbps).

Event Log Page

The Event Log page lists access point events and provides links to the Event Display Setup and Event Log Summary pages. You can also open Station pages for devices listed in the event log. Figure 13-9 shows an Event Log page example.

Figure 13-9 Event Log Page

Home Map Network Associations Setup **Logs** Help Uptime: 03:26:14

Index Number of Events [Download Event Log](#)

Press to Change Settings:

Event Log <i>additional display filters</i>		
Time	Severity	Description
03:26:08	Info	Station Joe Smith Associated
03:26:08	Info	Station Joe Smith Authenticated
03:25:23	Info	Station 209.165.201.7 Reassociated
03:25:21	Info	Disassociating 209.165.201.7 , reason "Sender is Leaving (has left) BSS"

40914

Click the **Logs** link at the top of any main management system page to reach the Event Log page.

Display Settings

Use the entry fields and the buttons at the top of the page to control the event list. Fields and buttons include:

- Index—Specifies the first event to display in the event list. The most recent event is 0; earlier events are numbered sequentially. To apply your entry, click **Apply New**.
- Number of Events—Specifies the number of events displayed on the page. To apply your entry, click **Apply New**.
- Next—Displays earlier events in the log.
- Prev—Displays more recent events in the log.

- **Apply New**—Changes the display by applying the settings in the Index and Number of Events fields.
- **Purge Log**—Permanently deletes all events from the log.
- **Additional Display Filters**—A link to the Event Display Setup page, where you can change time and severity level settings.

Log Headings

The event log is divided into three columns:

- **Time**—The time the event occurred. The log records time as cumulative days, hours, and minutes since the access point was turned on, or as wall-clock time if a time server is specified or if the time has been manually set on the access point.
- **Severity**—Events are classified as one of four severity levels depending on the event's impact on network operations. Severity levels include:
 - **Info (green)**—Indicates routine information; no error.
 - **Warning (blue)**—Indicates a potential error condition.
 - **Alert (magenta)**—Indicates that an event occurred which was pre-selected as something to be recorded in the log. A typical example of an alert would be a packet error condition. The Station page provides check boxes that activate reporting of packet errors to and from the station as alerts in the event log.
 - **FATAL (red)**—An event which prevents operation of the port or device. For operation to resume, the port or device usually must be reset.

Click the **Severity** heading to go to the Event Log Summary page, which lists total events for each severity level.

- **Description**—This column describes the nature or source of the event. If a network device is involved in the event, the device's MAC or IP address appears and provides a direct link to the device's Station page.

Saving the Log

To save the event log, click **Download Event Log**. In Microsoft Explorer, the log is saved as a text file. In Netscape Communicator, the log file is displayed on the screen, and you select **Save As** from Communicator's File pull-down menu to save the log.

Event Log Summary Page

The Event Log Summary page lists the total number of events that occurred at each severity level. [Figure 13-10](#) shows an Event Log Summary page example.

Figure 13-10 Event Log Summary Page

Home Map Network Associations Setup Logs Help							Uptime: 03:27:11
Event Severity Level							Total Events
System Fatal							0
Protocol Fatal							0
Network Port Fatal							0
System Alert							0
Protocol Alert							0
Network Port Alert							0
External Alert							0
System Warning							0
Protocol Warning							2
Network Port Warning							0
External Warning							0
System Information							0
Protocol Information							21
Network Port Information							21
External Information							1

4/29/15

Click the **Severity** heading on the Event Log page to reach the Event Log Summary page.

Using Command-Line Diagnostics

You can view diagnostic information about your access point with diagnostic commands. Enter the commands in the command-line interface (CLI) to display the information. You can open the CLI with Telnet or with a terminal emulator through the access point's serial port.

Table 13-1 lists the access point's diagnostic commands. Click a command in the left column to go to a description of that command's results.

Table 13-1 CLI Diagnostic Commands

Command	Information Displayed
:eap_diag1_on	Authentication progress for client devices authenticating through the access point
:eap_diag2_on	Packet contents of each authentication step for client devices authenticating through the access point
:vxdiag_arps	The ARP table
:vxdiag_checkstack	Task stack on the access point
:vxdiag_hostshow	Remote host list with IP addresses and aliases
:vxdiag_i	Task list on the access point

Table 13-1 CLI Diagnostic Commands (continued)

Command	Information Displayed
<code>:vxdiag_ipstatshow</code>	IP statistics
<code>:vxdiag_memshow</code>	Free and allocated memory on the access point
<code>:vxdiag_muxshow</code>	Networking protocols installed on the access point
<code>:vxdiag_routeshow</code>	Current routing information
<code>:vxdiag_tcpstatshow</code>	TCP statistics
<code>:vxdiag_udpstatshow</code>	UDP statistics

Entering Diagnostic Commands

Follow these steps to enter diagnostic commands in the CLI:


Note

These steps describe opening the CLI with Telnet. If the access point is configured to block Telnet access, follow the instructions in the “[Preparing to Use a Terminal Emulator](#)” section on page 2-4 to open the CLI by using a terminal emulator through a serial cable connected to the access point’s serial port.

Step 1

On your computer’s Start menu, select **Programs > Accessories > Telnet**.

If Telnet is not listed in your Accessories menu, select **Start > Run**, enter **Telnet** in the entry field, and press **Enter**.

Step 2

When the Telnet window appears, click **Connect**, and select **Remote System**.


Note

In Windows 2000, the Telnet window does not contain pull-down menus. To start the Telnet session in Windows 2000, enter **open** followed by the access point’s IP address.

Step 3

In the Host Name field, enter the access point’s IP address and click **Connect**.

Step 4

Press **=** to display the access point’s home page.

Step 5

Enter the command (for example, `:vxdiag_memshow`) and press **Enter**. The command’s diagnostic information appears.

Diagnostic Command Results

This section describes the information displayed on the CLI for the diagnostic commands listed in [Table 13-1](#).

:eap_diag1_on

Use the **:eap_diag1_on** command to display authentication progress for client devices authenticating through the access point. The steps in a successful authentication for a client device named Yakima might look like the following example:

```
EAP: Sending Identity Request
EAP: Received packet from Yakima
EAP: Received Identity Response
EAP: Forwarding packet to RADIUS server
RADIUS: Received packet for client Yakima
RADIUS: Received Challenge Request
RADIUS: Sending EAPOL packet to client
EAP: Received packet from Yakima
EAP: Forwarding packet to RADIUS server
RADIUS: Received packet for client Yakima
RADIUS: Received session timeout request of 60 seconds
RADIUS: Sending EAPOL packet to client
RADIUS: ACCEPT for Yakima
RADIUS: Found Cisco key
RADIUS: Sending EAPOL multicast key
RADIUS: Sending EAPOL session key parameters
EAP: Key set for client Yakima
```

The EAP and RADIUS prefixes show which system process is handling the communication.

Follow the steps in the “[Entering Diagnostic Commands](#)” section on page 13-16 to open the CLI and enter the **:eap_diag1_on** command.

:eap_diag2_on

Use the **:eap_diag2_on** command to display the packet contents of each authentication step for client devices authenticating through the access point. The packet contents for one authentication step might look like this example:

```
EAP: Sending Identity Request
00c15730: 01 00 00 28 01 21 00 28 01 00 6e 65 74 77 6f 72 *...(!(..networ*
00c15740: 6b 69 64 3d 45 41 50 33 2c 6e 61 73 69 64 3d 45 *kid=EAP3,nasid=E*
00c15750: 41 50 33 2c 70 6f 72 74 69 64 3d 30 *AP3,portid=0....*
```

The first group of characters in the packet contents (*00c15730*, for example) is the hexadecimal address of the memory buffer that contains the packet. The middle group of characters (*01 00 00 28 01 21 00 28 01 00 6e 65 74 77 6f 72*, for example) is the packet contents in hexadecimal format. The last group of characters (**...(!(..networ**, for example) is an ASCII representation of the packet contents.

For information on interpreting the content of packets sent between the access point and the RADIUS server, refer to the Internet Society’s *RFC 2865*. This document is available at <http://www.armware.dk/RFC/rfc/rfc2865.html> as well as on many other websites. The IEEE’s 802.1X authentication standard helps define the content of packets sent between client devices and the access point and is available to IEEE members at <http://www.ieee.org>.

Follow the steps in the “[Entering Diagnostic Commands](#)” section on page 13-16 to open the CLI and enter the **:eap_diag2_on** command.

:vxdiag_arpshow

Use the **:vxdiag_arpshow** command to display the access point's ARP table. The ARP table might look like the following example:

```
LINK LEVEL ARP TABLE
destination      gateway          flags  Refcnt  Use  Interface
-----
10.84.139.129    00:05:31:d3:c0:9  405   1       0   emac0
-----
```

These are descriptions for each column in the ARP table:

- Destination—IP address of the host entry
- Gateway—MAC address of the destination
- Flags—see [Table 13-2](#) for a list of flags

Table 13-2 Flag Definitions

Flag Value	Definition
0x1	Route is usable.
0x2	Destination is a gateway.
0x4	Host of specific routing entry.
0x8	Host or net is unreachable.
0x10	Created dynamically (by redirect).
0x20	Modified dynamically (by redirect).
0x40	Message confirmed.
0x80	Subnet mask is present.
0x100	Generate new routes on use.
0x200	External daemon resolves name.
0x400	Generated by ARP.
0x800	Manually added (static).
0x1000	Just discard packets (during updates).
0x2000	Modified by management protocol.
0x4000	Protocol-specific routing flag.
0x8000	Protocol-specific routing flag.

- Refcnt—the number of hosts referencing this address
- Use—number of packets forwarded
- Interface—one of four possible interfaces:
 - *emac0* for Ethernet
 - *awc0* for internal radio
 - *awc1* for external radio
 - *lo0* for internal loopback

Follow the steps in the “[Entering Diagnostic Commands](#)” section on page 13-16 to open the CLI and enter the `:vxdiag_arpshow` command.

`:vxdiag_checkstack`

Use the `:vxdiag_checkstack` command to display a summary of the stack activity for each access point task. A portion of the task stack might look like this example:

NAME	ENTRY	TID	SIZE	CUR	HIGH	MARGIN
tExcTask	0x00001a1fd0	fd4e80	7984	224	960	7024
tSysIntegrit	0x000001b188	a3b1c0	16368	720	1176	15192
tLogEventMgr	0x00000fb0ac	fd22d8	16368	2136	3616	12752
tShell	0x0000041da8	a2eb78	19320	640	2712	16608
tTelnetd	0x000002e220	a32d90	16368	376	1472	14896
tTelnetOutTa	0x000002e7fc	993da0	16368	720	1800	14568
tTelnetInTas	0x000002e858	98fb88	16368	1416	2376	13992

These are the descriptions of the information in each column:

- Name—name of the task
- Entry—entry point; the top-level function of the task
- TID—task identifier; the task control block
- Size—stack size in bytes
- CUR—current number of bytes of stack in use
- High—highest number of bytes of stack which have been in use
- Margin—the difference between the stack size and the highest number of bytes which have been in use

Follow the steps in the “[Entering Diagnostic Commands](#)” section on page 13-16 to open the CLI and enter the `:vxdiag_checkstack` command.

`:vxdiag_hostshow`

Use the `:vxdiag_hostshow` command to display remote hosts and their IP addresses and aliases. The remote host information might look like this example:

```
Clock: 96470 sec

hostname                ttl      inet address      aliases
-----                ---      -
localhost                0        127.0.0.1
10.84.139.161            7273     10.84.139.161
10.84.139.136            7273     10.84.139.136
10.84.139.138            7273     10.84.139.138
10.84.139.167            7273     10.84.139.167
10.84.139.160            7273     10.84.139.160
10.84.139.137            7273     10.84.139.137
AP_North.cisco.com      93073    10.84.139.135
10.84.139.164            7273     10.84.139.164
10.84.139.169            7274     10.84.139.169
10.84.139.141            97062    10.84.139.141
```

These are descriptions for the information in each column:

- Hostname—Domain name of the host, if available; otherwise, same as the Inet address
- TTL—time-to-live
- Inet address—IP address of the host
- Aliases—List of additional names, other than the hostname, that refer to the Inet address

Follow the steps in the “[Entering Diagnostic Commands](#)” section on page 13-16 to open the CLI and enter the `:vxdiag_hostshow` command.

`:vxdiag_i`

Use the `:vxdiag_i` command to display a list of current tasks on the access point. A portion of the access point’s task list display might look like this example:

NAME	ENTRY	TID	PRI	STATUS	PC	SP	ERRNO	DELAY
tExcTask	1a1fd0	fd4e80	0	PEND	1d9aac	fd4da0	3006b	0
tSysIntegrilb188		a3b1c0	0	SUSPEND	1c06ac	a3aef0	0	0
tLogEventMgfb0ac		fd22d8	1	PEND	1bcda8	fd1a80	0	0
tShell	41da8	a2eb78	1	PEND	1bcda8	a2e8f8	9	0
tTelnetd	2e220	a32d90	2	PEND	1bcda8	a32c18	0	0
tTelnetOutT2e7fc		993da0	2	PEND	1bcda8	993ad0	0	0
tTelnetInTa2e858		98fb88	2	PEND	1bcda8	98f600	3d0002	0
tBrowser	1351c8	a0d978	5	READY	1c2014	a0c4b8	3d0004	0
tIdleConsold274c		98b970	10	PEND	1bcda8	98b820	0	0
tThttpd	b435c	a5b3d8	45	PEND	1bcda8	a5b138	6b0003	0
tSNMPD	106fd8	b1eb80	46	PEND+T	1bcda8	b1d5b0	3d0004	1968

These are the descriptions of the information in each column:

- Name—name of the task
- Entry—entry point; the top-level function of the task
- TID—task identifier; the task control block
- PRI—task priority; a low number means a high priority
- Status—status of the task; five statuses are possible:
 - Pend—The task is in an inactive waiting state.
 - Pend+T—The task is waiting, but it has a timeout value for the length of time it will wait for an external event to wake the task and start it.
 - Suspend—The task will not begin until some external event occurs.
 - Ready—The task is ready to run.
 - Delay—The task issued a delay command and will not run until the delay time elapses.
- PC—program counter; a memory address of the task
- SP—stack pointer; another memory address of the task
- ERRNO—error number; the latest error reported by any function called by the task
- Delay—delay interval in system clock-ticks (1/52 second) that must elapse before the task runs

Follow the steps in the “[Entering Diagnostic Commands](#)” section on page 13-16 to open the CLI and enter the `:vxdiag_i` command.

:vxdiag_ipstatshow

Use the **:vxdiag_ipstatshow** command to display IP statistics for the access point. The IP statistics might look like the following example:

```
total 5760
badsum 0
tooshort 0
toosmall 0
badhlen 0
badlen 0
infragments 0
fragdropped 0
fragtimeout 0
forward 0
cantforward 0
redirectsent 0
unknownprotocol 0
nobuffers 0
reassembled 0
outfragments 0
noroute 0
```

These are descriptions of each IP statistic:

- Total—the total number of packets received
- Badsum—number of packets received with bad checksums
- Tooshort—number of packets received that were shorter than the expected length
- Toosmall—number of packets received that did not have enough data
- Badhlen—number of packets received with IP header length less than the packet data size
- Badlen—number of packets received with IP length less than the IP header length
- Infragments—number of packets received that were fragmented
- Fragdropped—number of fragmented packets received that were dropped
- Fragtimeout—number of fragmented packets received that timed out
- Forward—number of packets forwarded
- Cantforward—number of packets received for an unreachable destination
- Redirectsent—number of packets forwarded in the same subnet
- Unknownprotocol—number of packets received with unknown protocol information
- Nobuffers—number of packets dropped due to unavailable buffers
- Reassembled—number of packets reassembled successfully
- Outfragments—number of output fragments created
- Noroute—number of packets discarded due to no route available

Follow the steps in the [“Entering Diagnostic Commands”](#) section on page 13-16 to open the CLI and enter the **:vxdiag_ipstatshow** command.

:vxdiag_memshow

Use the **:vxdiag_memshow** command to display information on the access point's free and allocated memory. The access point's current memory information might look like the following example:

```

status   bytes      blocks  avg block  max block
-----  -
current
  free   7386392      476      15517    7296288
  alloc  6738808     10837      621         -
cumulative
  alloc 13483152   126889      106         -

```

These are descriptions for each information column:

- Status—the memory statuses described in the table, including current free memory, current allocated memory, and cumulative allocated memory, which is the total bytes and blocks of memory ever allocated by the access point
- bytes—the memory for each status described in bytes
- blocks—the memory for each status described in contiguous blocks; indicates the level of fragmentation in the access point's memory
- avg block—the average block size; simply put, the number in the bytes column divided by the number in the blocks column
- max block—the maximum contiguous memory block available

Follow the steps in the [“Entering Diagnostic Commands”](#) section on page 13-16 to open the CLI and enter the **:vxdiag_memshow** command.

:vxdiag_muxshow

Use the **:vxdiag_muxshow** command to display all the networking protocols installed on the access point. The list of installed protocols might look like the following example:

```

Device: emac Unit: 0
Description: PPC405GP Ethernet Media Access Controller Enhanced Network Driver
Protocol: AWC Packet Router      Type: 257      Recv 0x5ad0c    Shutdown 0x5fbd0
Protocol: Cisco Discovery Protocol (CDP)      Type: 8192     Recv 0x4f2c0
Shutdown 0x0
Protocol: AWC DDP Protocol        Type: 34605   Recv 0x6986c    Shutdown 0x6a728
Protocol: IP 4.4 ARP             Type: 2054    Recv 0x2732c    Shutdown 0x275ec
Protocol: IP 4.4 TCP/IP          Type: 2048    Recv 0x2732c    Shutdown 0x27524
Device: awc Unit: 0
Description: Aironet A504-Family Enhanced Network Driver
Protocol: AWC DDP Protocol        Type: 34605   Recv 0x6986c    Shutdown 0x6a728
Protocol: 802.1X Protocol        Type: 34958   Recv 0x9adc4    Shutdown 0x9e5a0
Protocol: AWC WNMP MAC-Level Control  Type: 34689   Recv 0x118af4   Shutdown
0x118e9c
Protocol: AWC 802.11 MAC-Level Control  Type: 57841   Recv 0x6c258    Shutdown
0x6c5dc
Protocol: AWC 802.11 MAC-Level Management  Type: 57840   Recv 0x6abf0
Shutdown 0x6c580
Protocol: AWC Packet Router      Type: 511     Recv 0x5ad0c    Shutdown 0x5fbd0
Device: rprr Unit: 1
Description: Aironet 802.11 Bridge Driver
Protocol: AWC Packet Router      Type: 257     Recv 0x5ad0c    Shutdown 0x5fbd0
Protocol: AWC DDP Protocol       Type: 34605   Recv 0x6986c    Shutdown 0x6a728
Device: rprr Unit: 2

```

Follow the steps in the “[Entering Diagnostic Commands](#)” section on page 13-16 to open the CLI and enter the `:vxdiag_muxshow` command.

`:vxdiag_routeshow`

Use the `:vxdiag_routeshow` command to display current routing information for the access point. The routing information might look like the following example:

```
ROUTE NET TABLE
destination      gateway          flags  Refcnt  Use    Interface
-----
0.0.0.0          10.84.139.129   3      1      1932   emac0
10.84.139.128    10.84.139.141  101    0        0     emac0
-----

ROUTE HOST TABLE
destination      gateway          flags  Refcnt  Use    Interface
-----
127.0.0.1        127.0.0.1       5      0      696    lo0
-----
```

These are descriptions for each column in the route net and route host tables:

- Destination—IP address of host to which access point is to be routed
- Gateway—IP address of host for forwarding packets not in the access point’s subnet
- Flags—see [Table 13-2](#) for a list of flags
- Refcnt—the number of hosts referencing this address
- Use—number of packets forwarded
- Interface—one of four possible interfaces:
 - `emac0` for Ethernet
 - `awc0` for internal radio
 - `awc1` for external radio
 - `lo0` for internal loopback

Follow the steps in the “[Entering Diagnostic Commands](#)” section on page 13-16 to open the CLI and enter the `:vxdiag_routeshow` command.

`:vxdiag_tcpstatshow`

Use the `:vxdiag_tcpstatshow` command to display Transmission Control Protocol (TCP) statistics for the access point. The TCP statistics might look like this example:

```
TCP:
  3370 packets sent
    1576 data packets (714752 bytes)
    3 data packets (1613 bytes) retransmitted
    1252 ack-only packets (1 delayed)
    0 URG only packet
    1 window probe packet
    0 window update packet
    538 control packets
  3327 packets received
    1564 acks (for 710621 bytes)
    23 duplicate acks
    0 ack for unsent data
```

```

824 packets (189251 bytes) received in-sequence
8 completely duplicate packets (2562 bytes)
0 packet with some dup. data (0 byte duped)
74 out-of-order packets (0 byte)
0 packet (0 byte) of data after window
0 window probe
85 window update packets
0 packet received after close
0 discarded for bad checksum
0 discarded for bad header offset field
0 discarded because packet too short
63 connection requests
415 connection accepts
477 connections established (including accepts)
477 connections closed (including 410 drops)
0 embryonic connection dropped
1378 segments updated rtt (of 1399 attempts)
2 retransmit timeouts
    0 connection dropped by rexmit timeout
1 persist timeout
0 keepalive timeout
    0 keepalive probe sent
    0 connection dropped by keepalive
63 pcb cache lookups failed

```

Follow the steps in the “[Entering Diagnostic Commands](#)” section on page 13-16 to open the CLI and enter the `:vxdiag_tcpstatshow` command.

`:vxdiag_udpstatshow`

Use the `:vxdiag_udpstatshow` command to display User Datagram Protocol (UDP) statistics for the access point. The UDP statistics might look like this example:

```

UDP:
9244 total packets
9227 input packets
17 output packets
0 incomplete header
0 bad data length field
0 bad checksum
9211 broadcasts received with no ports
0 full socket
16 pcb cache lookups failed
0 pcb hash lookup failed

```

Follow the steps in the “[Entering Diagnostic Commands](#)” section on page 13-16 to open the CLI and enter the `:vxdiag_udpstatshow` command.

Tracing Packets

Use the packet tracing feature to view packets sent and received by the access point and by other wireless devices on your network. You can view packets sent to and received from a single wireless device or several wireless devices, or you can view all the packets sent and received through the access point’s Ethernet and radio ports.

The IEEE’s 802.1X authentication standard helps define the content of packets and is available to IEEE members at <http://www.ieee.org>.

For information on filtering packets, see the [“Filter Setup” section on page 5-2](#).

Reserving Access Point Memory for a Packet Trace Log File

You can save packet traces in a log file that you view or save, or you can view packets on the access point command-line interface without storing the traces in a log file. Use the instructions in this section to reserve access point memory for a packet trace log file. Use the instructions in the [“Tracing Packets for Specific Devices” section on page 13-25](#) and the [“Tracing Packets for Ethernet and Radio Ports” section on page 13-26](#) to select devices and ports to be traced.

Follow these steps to reserve access point memory for a packet trace log file:

-
- Step 1** Use the Event Handling Setup page to enter instructions for the size of the packets you want to monitor and the amount of memory the access point should set aside for packet data. Follow this link path to the Event Handling Setup page:
 - a. On the Summary Status page, click **Setup**.
 - b. On the Setup page, click **Event Handling** under Event Log.
 - Step 2** Enter the number of bytes the access point should store for each packet in the Maximum number of bytes stored per Alert packet entry field. If you want to see the entire contents of each packet, enter **1600**; if you want to see only the packet header, enter **64**.
 - Step 3** Enter the number of bytes of memory the access point should use for packet tracing in the Maximum memory reserved for Detailed Event Trace Buffer (bytes) entry field. If you want to create a detailed packet trace, for example, enter **1000000**; if you need a simple, less-detailed packet trace, for example, enter **100000**.
 - Step 4** Click **OK**. The access point reboots.

Now you need to enter settings for the wireless devices or network interfaces for which you want to trace packets. Follow the steps in the [“Tracing Packets for Specific Devices” section on page 13-25](#) or the [“Tracing Packets for Ethernet and Radio Ports” section on page 13-26](#) to select devices and ports to be monitored.

Tracing Packets for Specific Devices

Follow these steps to select specific devices for which you want to trace packets:

-
- Step 1** Browse to the access point’s Association Table. You can reach the Association Table by clicking **Current Associations** on the Summary Status page or by clicking the gray **Associations** button at the top of most management system pages.
 - Step 2** Find the wireless device for which you want to trace packets and click the device’s MAC address. The device’s Station page appears.
 - Step 3** On the device’s Station page, click the **alert** checkbox in the To Station header to trace packets sent to the device. Click the **alert** checkbox in the From Station header to trace packets the device sends.

**Note**

Copying packets into access point memory slows the access point's performance. When you finish tracing packets, deselect the alert checkboxes on the Station pages.

If you want the access point to trace packets all the time, reduce the impact on performance by selecting **Record** for the External Information setting on the Event Handling Setup page and select **Port Information** on the Event Display Setup page for the "Severity Level at which to display events immediately on the console" setting. With this configuration, the access point records packets in a log file but does not spend time instantly displaying packets on the CLI.

- Step 4** Click Refresh. Repeat these steps for each device for which you want to trace packets. The MAC addresses of devices you are tracing appear in red in the Association Table.

If you are ready to view packet data, skip to the "[Viewing Packet Trace Data](#)" section on page 13-27. If you want to trace all the packets sent through the access point's Ethernet and radio ports, follow the instructions in the "[Tracing Packets for Ethernet and Radio Ports](#)" section on page 13-26.

Tracing Packets for Ethernet and Radio Ports

Follow these steps to set up the access point's Ethernet or radio ports for packet tracing:

- Step 1** To trace all the packets sent and received through the access point's Ethernet or radio ports, browse to the Network Ports page. Browse to the Network Ports page by clicking **Current Associations** on the Summary Status page or by clicking the gray **Network** button at the top of most management system pages.
- Step 2** To trace packets sent or received through the access point's Ethernet port, click **Ethernet** in the yellow header row. To trace packets sent or received through the access point's radio port, click **AP Radio** in the yellow header row. The Ethernet Port or AP Radio Port page appears.
- Step 3** Click the **alert** checkbox in the Receive header to trace packets received through the Ethernet or radio port. Click the **alert** checkbox in the Transmit header to trace packets sent through the Ethernet or Radio port.

**Note**

Copying packets into access point memory slows the access point's performance. When you finish tracing packets, deselect the alert checkboxes on the Station pages.

If you want the access point to trace packets all the time, reduce the impact on performance by selecting **Record** for the External Information setting on the Event Handling Setup page and select **Port Information** on the Event Display Setup page for the "Severity Level at which to display events immediately on the console" setting. With this configuration, the access point records packets in a log file but does not spend time instantly displaying packets on the CLI.

- Step 4** Click **Refresh**. The network interface you are tracing appears in red on the Summary Status, Setup, and Network Ports pages.

- Step 5** Follow the steps in the "[Viewing Packet Trace Data](#)" section on page 13-27 to view the traced packets in a log file or on the CLI.

Viewing Packet Trace Data

If you store traced packets in a log file, you can view or save the file. If you do not store traced packets, you can view the packets in real time on the access point CLI.

Packets Stored in a Log File

Follow these steps to view traced packets stored in a log file:

- Step 1** Browse to the Event Handling Setup page. Follow this link path to the Event Handling Setup page:
 - a. On the Summary Status page, click **Setup**.
 - b. On the Setup page, click **Event Handling** under Event Log.
- Step 2** Click **Headers Only** to view only the packet headers; click **All Data** to view all the collected packet information.
- Step 3** A File Download window appears asking if you want to save the [access point name]_trace.log file or open it. Choose to save or open the file and click **OK**.

A portion of the Headers Only packet trace file might look like this example:

```
===Beginning of AP_North Detailed Trace Log===
04:46:14 +17174.384615 Station Alert: 00:01:64:43:ef:41Aironet:40:6f:e6Aironet:40:6f:e6 0x0000
04:47:37 + 83.326923 Station Alert: 00:01:64:43:ef:41Aironet:40:6f:e6Aironet:36:14:5a 0x0000
04:49:06 + 88.307692 Station Alert: 00:01:64:43:ef:41Aironet:40:6f:e6broadcastARP
04:49:06 + 0.000000 Station Alert: 00:05:31:d3:c0:0900:01:64:43:ef:41ARP
04:49:06 + 0.000000 Station Alert: 00:01:64:43:ef:41Aironet:40:6f:e600:05:31:d3:c0:09IP IPv4 UDP
ID=0x14f2 totalLen=96 10.84.139.164 -> ne-wins.cisco.com
04:49:06 + 0.230769 Station Alert: 00:05:31:d3:c0:0900:01:64:43:ef:41IP IPv4 UDP ID=0xb0b4 totalLen=90
ne-wins.cisco.com -> 10.84.139.164
04:49:06 + 0.019231 Station Alert: 00:01:64:43:ef:41Aironet:40:6f:e600:05:31:d3:c0:09IP IPv4 UDP
ID=0x14f3 totalLen=96 10.84.139.164 -> ne-wins.cisco.com
04:49:06 + 0.192308 Station Alert: 00:05:31:d3:c0:0900:01:64:43:ef:41IP IPv4 UDP ID=0xb2b4 totalLen=90
ne-wins.cisco.com -> 10.84.139.164
===End of AP_North Detailed Trace Log===
```

A portion of the All Data packet trace file might look like this example:

```
===Beginning of AP_North Detailed Trace Log===
04:46:14 +17174.384615 Station Alert: 00:01:64:43:ef:41[Aironet]00:40:96:40:6f:e6[Aironet]00:40:96:40:6f:e6
0x0000
 00 4a 40 81 00 40 96 40 6f e6 00 01 64 43 ef 41 01 7f 00 04 5f 00 00 40 96 40 6f e6 00 00 00 00 00 00
00 00 0a 54 8b a4 00 00 44 57 49 4c 4c 2d 49 42 4d 2d 57 32 4b 00 00 00 00 00 00 00 00 00
|.J@..@.o...dC.A..._..@.o.....T...JCOOL-IBM-W2K.....|
04:47:37 + 83.326923 Station Alert: 00:01:64:43:ef:41[Aironet]00:40:96:40:6f:e6[Aironet]00:40:96:36:14:5a
0x0000
 00 4a 40 81 00 40 96 36 14 5a 00 01 64 43 ef 41 01 7f 00 04 5f 00 00 40 96 40 6f e6 00 00 00 00 00 00
00 00 0a 54 8b a4 00 00 44 57 49 4c 4c 2d 49 42 4d 2d 57 32 4b 00 00 00 00 00 00 00 00 00
|.J@..@.6.Z..dC.A..._..@.o.....T...JCOOL-IBM-W2K.....|
===End of AP_North Detailed Trace Log===
```

Packets Displayed on the CLI

To view packets displayed on the access point CLI, follow the instructions in the [“Using the Command-Line Interface”](#) section on page 2-4 to open the CLI. The access point displays the packets at the bottom of the screen.

Checking the Top Panel Indicators

If your access point is not communicating, check the three indicators on the top panel. The indicators report the unit’s status. [Figure 13-11](#) shows the indicators on an access point with a plastic case, and [Figure 13-12](#) shows the indicators on an access point with a metal case. [Table 13-3](#) lists the meanings of the indicator signals.

Figure 13-11 Indicator Lights on Access Point with Plastic Case

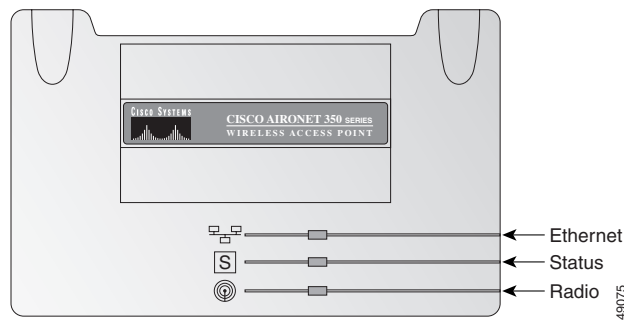
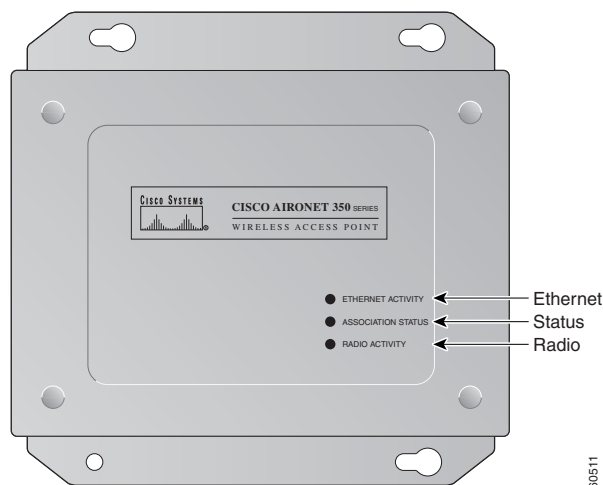


Figure 13-12 Indicator Lights on Access Point with Metal Case



- The Ethernet indicator signals traffic on the wired LAN, or Ethernet infrastructure. This indicator blinks green when a packet is received or transmitted over the Ethernet infrastructure.

- The status indicator signals operational status. Blinking green indicates that the access point is operating normally but is not associated with any wireless devices. Steady green indicates that the access point is associated with a wireless client.

For repeater access points, blinking 50% on, 50% off indicates the repeater is not associated with the root access point; blinking 7/8 on, 1/8 off indicates that the repeater is associated with the root access point but no client devices are associated with the repeater; steady green indicates that the repeater is associated with the root access point and client devices are associated with the repeater.

- The radio indicator blinks green to indicate radio traffic activity. The light is normally off, but it blinks green whenever a packet is received or transmitted over the access point's radio.

Table 13-3 Top Panel Indicator Signals

Message type	Ethernet indicator	Status indicator	Radio indicator	Meaning
Association status	–	Steady green	–	At least one wireless client device is associated with the unit.
	–	Blinking green	–	No client devices are associated; check the unit's SSID and WEP settings.
Operational	–	Steady green	Blinking green	Transmitting/receiving radio packets.
	Blinking green	Steady green	–	Transmitting/receiving packets.
	–	Steady green	Blinking amber	Maximum retries or buffer full occurred on the radio.
Error/warning	Blinking amber	Steady green	–	Transmit/receive errors.
	Blinking red	–	–	Ethernet cable is disconnected (340 series only).
	–	Blinking amber	–	General warning.
Failure	Steady red	Steady red	Steady red	Firmware failure; disconnect power from the unit and reapply power.
Firmware upgrade	–	Steady red	–	Unit is loading new firmware.

Finding an Access Point by Blinking the Top Panel Indicators

If you need to find the physical location of a particular access point, you can put the top panel indicators into blinking mode. Follow these instructions to blink the access point's top panel indicators:

-
- Step 1** Browse to the access point's Cisco Services Setup page:
- On the Summary Status page, click **Setup**.
 - On the Setup page, click **Cisco Services**.
- Step 2** Select **Enabled** for the Locate unit by flashing LEDs option.
- Step 3** Click **Apply**. The access point's top panel indicators blink amber in unison.
- Step 4** To make the indicators stop blinking and return to normal operation, select **Disabled** for the Locate unit by flashing LEDs option, and click **Apply**.
-

Checking Basic Settings

Mismatched basic settings are the most common causes of lost connectivity with wireless clients. If the access point does not communicate with client devices, check the following settings.

SSID

Wireless clients attempting to associate with the access point must use the same SSID as the access point. The default SSID is tsunami.

WEP Keys

The WEP key you use to transmit data must be set up exactly the same on your access point and any wireless devices with which it associates. For example, if you set WEP Key 3 on your wireless LAN adapter to 0987654321 and select it as the transmit key, you must also set WEP Key 3 on the access point to exactly the same value. The access point does not need to use Key 3 as its transmit key, however.

**Note**

If you use Network-EAP as the authentication type, you must select key 1 as the access point's transmit key. The access point uses the WEP key you enter in key slot 1 to encrypt multicast data signals it sends to EAP-enabled client devices. Because the access point transmits the WEP key used for multicast messages to the EAP-enabled client device during the EAP authentication process, that key does not have to appear in the EAP-enabled device's WEP key list. The access point uses a dynamic WEP key to encrypt unicast messages to EAP-enabled clients.

Refer to the [“Setting Up WEP” section on page 8-7](#) for instructions on setting the access point's WEP keys.

EAP Authentication Requires Matching 802.1X Protocol Drafts

**Note**

This section applies to wireless networks set up to use LEAP. If you do not use LEAP on your wireless network, you can skip this section.

Wireless client devices use Extensible Authentication Protocol (EAP) to log onto a network and generate a dynamic, client-specific WEP key for the current logon session. If your wireless network uses WEP without EAP, client devices use the static WEP keys entered in the Aironet Client Utilities.

If you use Network-EAP authentication on your wireless network, your client devices and access points must use the same 802.1X protocol draft. For example, if the radio firmware on the client devices that will associate with an access point or bridge is 4.16, then the access point or bridge should be configured to use Draft 8 of the 802.1X protocol. Table 13-4 lists firmware versions for Cisco Aironet products and the draft with which they comply.

Table 13-4 802.1X Protocol Drafts and Compliant Client Firmware

Firmware Version	Draft 7	Draft 8	Draft 10
PC/PCI cards 4.13	—	x	—
PC/PCI cards 4.16	—	x	—
PC/PCI cards 4.23	—	x	—
PC/PCI cards 4.25 and later	—	—	x
WGB34x/352 8.58	—	x	—
WGB34x/352 8.61 or later	—	—	x
AP34x/35x 11.05 and earlier	—	x	—
AP34x/35x 11.06 and later ¹	—	x	x
BR352 11.06 and later ¹	—	x	x

1. The default draft setting in access point and bridge firmware version 11.06 and later is Draft 10.



Note

Draft standard 8 is the default setting in firmware version 11.05 and earlier, and it might remain in effect when you upgrade the firmware to version 11.06 or later. Check the setting on the Authenticator Configuration page in the management system to make sure the best draft standard for your network is selected.

Use the Authenticator Configuration page to select the draft of the 802.1X protocol the access point's radio should use. Follow these steps to set the draft for your access point:

-
- Step 1** Browse to the Authenticator Configuration page in the access point management system.
- On the Summary Status page, click **Setup**.
 - On the Setup page, click **Security**.
 - On the Security Setup page, click **Authentication Server**.
- Step 2** Use the 802.1X Protocol Version (for EAP authentication) pull-down menu to select the draft of the 802.1X protocol the access point's radio should use. Menu options include:
- Draft 7—No radio firmware versions compliant with Draft 7 have LEAP capability, so you should not need to select this setting.
 - Draft 8—Select this option if LEAP-enabled client devices that associate with this access point use radio firmware versions 4.13, 4.16, or 4.23.

- **Draft 10**—This is the default setting in access point firmware versions 11.06 and later. Select this option if client devices that associate with this access point use Microsoft Windows XP EAP authentication or if LEAP-enabled client devices that associate with this bridge use radio firmware version 4.25 or later.

Step 3 Click **Apply** or **OK** to apply the setting. The access point reboots.

Resetting to the Default Configuration

If you forget the password that allows you to configure the access point, you might need to completely reset the configuration. Follow the steps below to delete the current configuration and return all access point settings to the factory defaults.

Steps for Firmware Versions 11.07 or Later

Follow the steps in this section if your access point is running firmware version 11.07 or later.



Note

The following steps reset *all* configuration settings to factory defaults, including passwords, WEP keys, the IP address, and the SSID. If you do not need to reset the entire configuration, use the Configuration Reset buttons on the System Configuration Setup page in the web-browser interface. Consult the [“Resetting the Configuration” section on page 10-13](#) for more information on the reset buttons in the web-browser interface.

Step 1 Use a straight-through cable with 9-pin male to 9-pin female connectors to connect the COM 1 or COM 2 port on your computer to the RS-232 port on the access point.

Step 2 Open a terminal-emulation program on your computer.



Note These instructions describe HyperTerminal; other programs are similar.

Step 3 In the Connection Description window, enter a name and select an icon for the connection and click **OK**.

Step 4 In the Connect To window, select the port to which the cable is connected and click **OK**.

Step 5 In the Port Settings window, enter the following settings:

- **9600** baud,
- **8** data bits,
- **No** parity,
- **1** stop bit, and
- **Xon/Xoff** flow control

Step 6 Click **OK**, and press **Enter**.

Step 7 When the Summary Status screen appears, reboot the access point by unplugging the power connector and then plugging it back in.

Step 8 When the access point reboots and the Summary Status screen reappears, type **:resetall**, and press **Enter**.

Step 9 Type **yes**, and press **Enter** to confirm the command.



Note The **resetall** command is valid for only 2 minutes immediately after the access point reboots. If you do not enter and confirm the **resetall** command during that 2 minutes, reboot the access point again.

Step 10 After the access point reboots and the Express Setup screen appears, reconfigure the access point by using the terminal emulator or an Internet browser.

Steps for Firmware Versions 11.06 or Earlier

Follow the steps in this section if your access point is running firmware version 11.06 or earlier.



Note The following steps reset *all* configuration settings to factory defaults, including passwords, WEP keys, the IP address, and the SSID. If you do not need to reset the entire configuration, use the Configuration Reset buttons on the System Configuration Setup page in the web-browser interface. Consult the [“Resetting the Configuration” section on page 10-13](#) for more information on the reset buttons in the web-browser interface.

Determining the Boot-Block Version

The steps you follow to reconfigure the access point depend on the version of the access point’s boot block. Follow these steps to find out which boot block version is on your access point:

Step 1 Open a Telnet session to the access point.



Note You can also use these instructions while communicating with the access point through the console port or with an SNMP manager. Skip to [Step 3](#) if you use an SNMP manager.

Step 2 Type **:cmd** and press **Enter** to switch from text-browser mode to SNMP mode.

Step 3 Type **bootblockVersion** and press **Enter**. Text appears with information about the system. If your access point’s boot block version is 1.01, the text might look like this:

```
OID: iso.org.dod.internet.private.enterprises.aironet.awcVx.awcSystem.  
bootblockVersion  
Value [RO]: 1.01
```

Step 4 Type **exit** and press **Enter** to return to text-browser mode.

Step 5 If your boot block version is 1.01 or earlier, follow the instructions in the [“Reconfiguration Steps for Boot Block Version 1.01 or Earlier” section on page 13-34](#). If your boot block version is 1.02 or later, follow the instructions in the [“Reconfiguration Steps for Boot Block Version 1.02 or Later” section on page 13-35](#).

Reconfiguration Steps for Boot Block Version 1.01 or Earlier

Follow these steps to reconfigure your access point if the boot block version on your access point is version 1.01 or earlier and the firmware version on your access point is 11.06 or earlier. To find which boot block version is on your access point, follow the steps in the [“Determining the Boot-Block Version” section on page 13-33](#).



Caution

Failure to follow these instructions correctly can result in a nonoperational access point that must be returned to the factory. If your access point stops working after you attempt this procedure, contact Cisco TAC for assistance.

Step 1 Use a straight-through cable with 9-pin male to 9-pin female connectors to connect the COM 1 or COM 2 port on your computer to the RS-232 port on the access point.

Step 2 Open a terminal-emulation program on your computer.



Note

These instructions describe HyperTerminal; other programs are similar.

Step 3 In the Connection Description window, enter a name and select an icon for the connection and click **OK**.

Step 4 In the Connect To window, select the port to which the cable is connected and click **OK**.

Step 5 In the Port Settings window, make the following settings: **9600** baud, **8** data bits, **No** parity, **1** stop bit, and **Xon/Xoff** flow control.

Step 6 Click **OK** and press **Enter** three times.

Step 7 When the Summary Status screen appears, reboot the access point by unplugging the power connector and then plugging it back in, or by pressing **Ctrl-X**.

Step 8 When the message “Type <esc> within 5 seconds for menu” appears, press **Esc**.

Step 9 Write down the list of files for future reference.



Caution

Perform the next six steps carefully to avoid accidentally deleting the installation key files or the firmware files. You must carefully note the file selection letters, because they change during the following steps. If you forget to copy the access point’s installation key file to DRAM in [Step 10](#), or if you do not copy it back to configuration memory in [Step 13](#), your access point will stop functioning.

Step 10 Copy the access point’s installation key file to the access point’s DRAM by pressing **c** to select **Copy file**, then **1** to select **DRAM**, then the selection letter for the file called *AP Installation Key*.

Step 11 If the list of configuration files contains a file called *VAR Installation Key*, copy that file to DRAM along with the AP Installation Key. Copy the VAR installation key file to DRAM by pressing **c** to select **Copy file**, then **1** to select **DRAM**, then the selection letter for the file called *VAR Installation Key*.



Caution

Make sure you select the Configuration memory bank for formatting in [Step 12](#). If you accidentally format a different memory bank your access point will stop functioning.

Step 12 Reformat the access point’s configuration memory bank by pressing **!** to select **FORMAT memory bank**, then **2** to select **Config**, then upper-case **Y** to confirm the **FORMAT** command.

- Step 13** Copy the installation key back to the configuration memory bank by pressing **c** to select **Copy file**, then **2** to select **Config**, then the selection letter for the AP Installation Key.
- Step 14** If you copied a VAR installation key to DRAM in [Step 11](#), copy it back to the configuration memory bank by pressing **c** to select **Copy file**, then **2** to select **Config**, then the selection letter for the file *VAR Installation Key*. If the access point does not have a VAR installation key file, skip to [Step 15](#).
- Step 15** Run the access point firmware by pressing **r** to select **Run**, then the selection letter for the firmware file which is displayed. The message “Inflating [firmware file name]” appears while the access point starts the firmware.
- Step 16** When the Express Setup screen appears, begin reconfiguring the access point using the terminal emulator or an Internet browser.
-

Reconfiguration Steps for Boot Block Version 1.02 or Later

Follow these steps to reconfigure your access point if the boot block version on your access point is version 1.02 or later and the firmware version on your access point is 11.06 or earlier. To find which boot block version is on your access point, follow the steps in the [“Determining the Boot-Block Version” section on page 13-33](#).



Caution

Failure to follow these instructions correctly can result in a nonoperational access point that must be returned to the factory. If your access point stops working after you attempt this procedure, contact Cisco TAC for assistance.

- Step 1** Use a straight-through cable with 9-pin male to 9-pin female connectors to connect the COM 1 or COM 2 port on your computer to the RS-232 port on the access point.
- Step 2** Open a terminal-emulation program on your computer.



Note

These instructions describe HyperTerminal; other programs are similar.

- Step 3** In the Connection Description window, enter a name and select an icon for the connection and click **OK**.
- Step 4** In the Connect To window, select the port to which the cable is connected and click **OK**.
- Step 5** In the Port Settings window, make the following settings: **9600** baud, **8** data bits, **No** parity, **1** stop bit, and **Xon/Xoff** flow control.
- Step 6** Click **OK** and press **Enter**.
- Step 7** When the Summary Status screen appears, reboot the access point by pressing **Ctrl-X** or by unplugging the power connector and then plugging it back in.
- Step 8** When the memory files are listed under the heading “Memory:File,” press **Ctrl-W** within 5 seconds to reach the boot block menu.
- Step 9** Write down the list of files for future reference.

**Caution**

Perform the next six steps carefully to avoid accidentally deleting the installation key files or the firmware files. You must carefully note the file selection letters, because they change during the following steps. If you forget to copy the access point's installation key file to DRAM in [Step 10](#), or if you do not copy it back to configuration memory in [Step 13](#), your access point will stop functioning.

Step 10 Copy the access point's AP Installation Key to the access point's DRAM by pressing **c** to select **Copy file**, then **1** to select **DRAM**, then the selection letter for the file *AP Installation Key*.

Step 11 If the list of configuration files contains a file called *VAR Installation Key*, you must copy that file to DRAM along with the AP Installation Key file. If the access point does not have a VAR installation key file, skip to [Step 12](#).

**Caution**

If you forget to copy the access point's VAR installation key file to DRAM in [Step 11](#), or if you do not copy it back to configuration memory in [Step 14](#), your access point will stop functioning.

Copy the VAR Installation Key to DRAM by pressing **c** to select **Copy file**, then **1** to select **DRAM**, then the selection letter for the file *VAR Installation Key*.

Step 12 Reformat the access point's configuration memory bank by pressing **Ctrl-Z** to reach the reformat menu. When the menu appears, press **!** to select **FORMAT memory bank**, then **2** to select **Config**, then upper-case **Y** to confirm the **FORMAT** command.

**Caution**

Make sure you select the Configuration memory bank for formatting. If you accidentally format a different memory bank your access point will stop functioning.

Step 13 Copy the installation key back to the configuration memory bank by pressing **c** to select **Copy file**, then **2** to select **Config**, then the selection letter for the file *AP Installation Key*.

Step 14 If you copied a VAR installation key to DRAM in [Step 11](#), copy it back to the configuration memory bank by pressing **c** to select **Copy file**, then **2** to select **Config**, then the selection letter for the file *VAR Installation Key*. If the access point does not have a VAR installation key file, skip to [Step 15](#).

Step 15 Run the access point firmware by pressing **r** to select **Run**, then the selection letter for the firmware file that is displayed. The message "Inflating [firmware file name]" appears while the access point starts the firmware.

Step 16 When the Express Setup screen appears, begin reconfiguring the access point using the terminal emulator or an Internet browser.