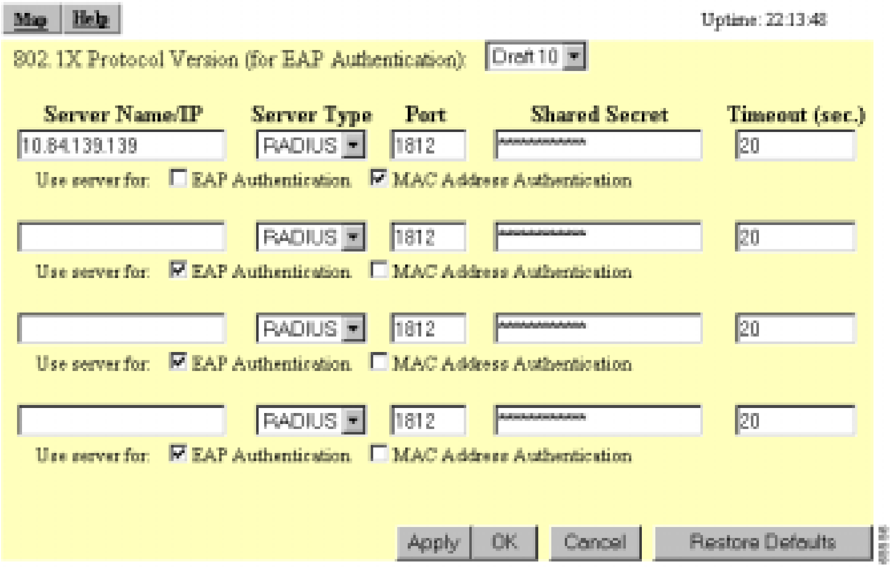
Step 4 If you plan to create a MAC address list that will be checked by the authentication server, select **Yes** for the option called Lookup MAC Address on Authentication Server if not in Existing Filter List. With this option enabled, the access point checks the authentication server's MAC address list when a client device attempts to authenticate.

Step 5 Click **Apply** to save the list of MAC addresses in the access point management system.

Step 6 Click the **Authentication Server** link to go to the Authenticator Configuration page. Figure 4-11 shows the Authenticator Configuration page.

Figure 4-11 Authenticator Configuration Page



Uptime: 22:13:48

802.1X Protocol Version (for EAP Authentication): Draft 10

Server Name/IP	Server Type	Port	Shared Secret	Timeout (sec.)
10.84.139.139	RADIUS	1812	**********	20
Use server for:	☐ EAP Authentication	☑ MAC Address Authentication		
	RADIUS	1812	**********	20
Use server for:	☑ EAP Authentication	☐ MAC Address Authentication		
	RADIUS	1812	**********	20
Use server for:	☑ EAP Authentication	☐ MAC Address Authentication		
	RADIUS	1812	**********	20
Use server for:	☑ EAP Authentication	☐ MAC Address Authentication		

You can configure up to four servers for authentication services, so you can set up backup authenticators. If you set up more than one server for the same service, the server first in the list is the primary server for that service, and the others are used in list order when the previous server times out.

Step 7 Enter the name or IP address of the authentication server in the Server Name/IP entry field.

Step 8 Enter the port number the server uses for authentication. The default setting, *1812*, is the port setting for Cisco's RADIUS server, the Cisco Secure Access Control Server (ACS), and for many other RADIUS servers. Check your server's product documentation to find the correct port setting.

Step 9 Enter the shared secret used by the server in the Shared Secret entry field. The shared secret on the bridge must match the shared secret on the server.

Step 10 Enter the number of seconds the access point should try contacting the primary authentication server in the Timeout entry field. If the primary authentication server does not respond within this time, the access point tries to contact the backup authentication server if one is specified.

Step 11 Select **MAC Address Authentication** under the server. If you set up a backup authentication server, select **MAC Address Authentication** under the backup server, also.

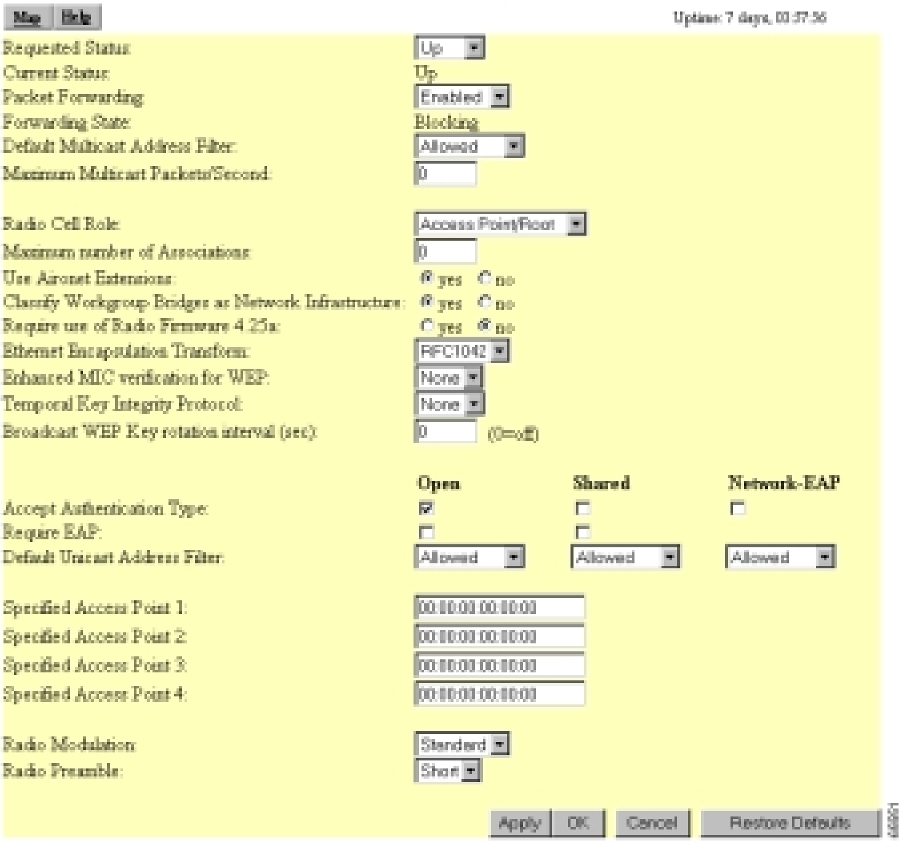
Step 12 Click **OK**. You return automatically to the Setup page.

Step 13 Create a list of allowed MAC addresses for your authentication server. Enter the MAC addresses of all allowed clients as users in the server's database. The "Enabling MAC-Based Authentication in Cisco Secure ACS" section on page 4-35 describes how to create a list of MAC addresses for your RADIUS server.

Note Be sure to include your own MAC address in the authentication server's list.

Step 14 Click **Advanced** in the AP Radio row of the Network Ports section at the bottom of the Setup page. The AP Radio Advanced page appears. Figure 4-12 shows the AP Radio Advanced page.

Figure 4-12 AP Radio Advanced Page



Uptime: 7 days, 03:37:56

Requested Status: Up

Current Status: Up

Packet Forwarding: Enabled

Forwarding State: Blocking

Default Multicast Address Filter: Allowed

Maximum Multicast Packets/Second: 0

Radio Cell Role: Access Point/Root

Maximum number of Associations: 0

Use Aironet Extensions: ● yes ○ no

Classify Workgroup Bridges as Network Infrastructure: ● yes ○ no

Require use of Radio Firmware 4.25a: ○ yes ● no

Ethernet Encapsulation Transform: RFC1042

Enhanced MIC verification for WEP: None

Temporal Key Integrity Protocol: None

Broadcast WEP Key rotation interval (sec): 0 (0=off)

	Open	Shared	Network-EAP
Accept Authentication Type:	☑	□	□
Require EAP:	□	□	
Default Unicast Address Filter:	Allowed	Allowed	Allowed

Specified Access Point 1: 00:00:00:00:00:00

Specified Access Point 2: 00:00:00:00:00:00

Specified Access Point 3: 00:00:00:00:00:00

Specified Access Point 4: 00:00:00:00:00:00

Radio Modulation: Standard

Radio Preamble: Short

Step 15 Select **Disallowed** from the pull-down menu for Default Unicast Address Filter for each authentication type requiring MAC-based authentication.

For example, if the access point is configured for both open and Network-EAP authentication, you could set Default Unicast Address Filter under Open to Disallowed but leave Default Unicast Address Filter under Network-EAP set to Allowed. This configuration forces client devices using open authentication to authenticate using MAC addresses but does not force LEAP-enabled client devices to authenticate using MAC addresses. To force all client devices to authenticate using MAC addresses, select **Disallowed** for all the enabled authentication types.

When you set Default Unicast Address Filter to disallowed, the access point discards all unicast traffic except packets sent to the MAC addresses listed as allowed on the authentication server or on the access point's Address Filters page.

Note Client devices associated to the access point are not immediately affected when you set Default Unicast Address Filter to disallowed.

Step 16 Click **OK**. You return automatically to the Setup page. Client devices that associate with the access point will not be allowed to authenticate unless their MAC addresses are included in the list of allowed addresses.

Authenticating Client Devices Using MAC Addresses or EAP

You can set up the access point to authenticate client devices using a combination of MAC-based and EAP authentication. When you enable this feature, client devices that associate to the access point using 802.11 open authentication first attempt MAC authentication. If MAC authentication succeeds, the client device joins the network; if the client is also using EAP authentication, it attempts to authenticate using EAP. If MAC authentication fails, the access point waits for the client device to attempt EAP authentication.

Follow these steps to combine MAC-based and EAP authentication for client devices using 802.11 open authentication:

Step 1 Follow the steps in the "Setting Up EAP Authentication" section on page 4-19 to set up EAP. You must select **Require EAP** under Open authentication on the AP Radio Data Encryption page to force client devices to perform EAP athentication if they fail MAC authentication. If you do not select **Require EAP**, client devices that fail MAC authentication might be able to join the network without performing EAP authentication.

Step 2 Follow the steps in the "Setting Up MAC-Based Authentication" section on page 4-29 to set up MAC-based authentication.

Step 3 Follow this link path to reach the Address Filters page:

a. On the Summary Status page, click **Setup**.

b. On the Setup page, click **Address Filters** under Associations.

Step 4 Select **yes** for the option called *Is MAC Authentication alone sufficient for a client to be fully authenticated?*

Step 5 Click **Apply**. When you enable this feature, the access point follows these steps to authenticate all clients that associate using 802.11 open authentication:

a. When a client device sends an authentication request to the access point, the access point sends a MAC authentication request in the RADIUS Access Request Packet to the RADIUS server using the client's user ID and password as the MAC address of the client.

b. If the authentication succeeds, the client joins the network. If the client is also using EAP authentication, it attempts to authenticate using EAP.

c. If MAC authentication fails for the client, the access point allows the client to attempt to authenticate using EAP authentication. The client cannot join the network until EAP authentication succeeds.

Enabling MAC-Based Authentication in Cisco Secure ACS

Cisco Secure Access Control Server for Windows NT/2000 Servers (Cisco Secure ACS) can authenticate MAC addresses sent from the access point. The access point works with ACS to authenticate MAC addresses using Secure Password Authentication Protocol (Secure PAP). You enter a list of approved MAC addresses into the ACS as users, using the client devices' MAC addresses as both the username and password. The authentication server's list of allowed MAC addresses can reside on the authentication server or at any network location to which the server has access.

Follow these steps to create a list of allowed MAC addresses in Cisco Secure ACS:

Step 1 On the ACS main menu, click **User Setup**.

Step 2 When the User text box appears, enter the MAC address you want to add to the list.

Note The access point sends MAC address queries to the server using lower-case characters. If your server allows case-sensitive usernames and passwords, you must enter MAC addresses in the server's database using lower-case characters.

Step 3 When the User Setup screen appears, enter the MAC address in the Cisco Secure PAP Password and Confirm Password entry fields.

Step 4 Enter the MAC address in the CHAP/MS-CHAP/ARAP Password and Confirm Password entry fields.

Step 5 Select the Separate (CHAP/MS-CHAP/ARAP) checkbox.

Step 6 Click **Submit**. Repeat these steps for each MAC address you want to add to the list of allowed MAC addresses.

MAC addresses that you enter in the authentication server's list appear in the access point's address filter list when the client device is associated to the access point. MAC addresses in the server's list disappear from the access point's list when the client devices disassociate or when the access point is reset.

Note Be sure to include your own MAC address in the authentication server's list to avoid losing connectivity to the access point.

Summary of Settings for Authentication Types

Table 4-5 lists the access point settings required to enable each authentication type and combinations of authentication types.

Table 4-5 Settings for Authentication Types

Authentication Types	Required Settings
LEAP	On the Authenticator Configuration page (shown in Figure 4-13): • Select an 802.1x protocol draft that matches the protocol draft used by client devices that associate with the access point. • Enter the name or IP address, type, port, shared secret, and timeout value for your RADIUS server. • Select the **EAP** checkbox under the server. On the AP Radio Data Encryption page (shown in Figure 4-6): • Select the **Network-EAP** checkbox. • Enter a WEP key in key slot 1 and select **128-bit** from the key size menu.
LEAP and static WEP under 802.11 Open	• Enter all the settings for LEAP authentication. On the AP Radio Data Encryption page (shown in Figure 4-6): • Select the **Open** checkbox.

Table 4-5 Settings for Authentication Types (continued)

Authentication Types	Required Settings
EAP-TLS and EAP-MD5	On the Authenticator Configuration page (shown in Figure 4-13): • Select an 802.1x protocol draft that matches the protocol draft used by client devices that associate with the access point. • Enter the name or IP address, type, port, shared secret, and timeout value for your RADIUS server. • Select the **EAP** checkbox under the server. On the AP Radio Data Encryption page (shown in Figure 4-6): • Select the **Open** and **Network-EAP** checkboxes. • Select the **Require EAP** checkbox under Open. **Note** Selecting **Require EAP** blocks non-EAP client devices from using the access point. • Enter a WEP key in key slot 1 and select **128-bit** from the key size pull-down menu.
EAP-TLS, EAP-MD5, and static WEP under 802.11 Open	The access point does not support this combination of authentication types. When you select **Require EAP** on the Authenticator Configuration page to authenticate clients using EAP-TLS and EAP-MD5, non-EAP client devices are blocked from using the access point. However, the access point can serve client devices using 802.11 open authentication if the access point is set up for MAC-based authentication and EAP authentication. See the "Authenticating Client Devices Using MAC Addresses or EAP" section on page 4-34 for instructions on setting up this combination of authentications.

Table 4-5 Settings for Authentication Types (continued)

Authentication Types	Required Settings
MAC-based	On the Address Filters page (shown in Figure 4-10): - Select **yes** for the "Look up MAC address on authentication server if not in existing filter list" setting. On the Authenticator Configuration page (shown in Figure 4-13): - Select an 802.1x protocol draft that matches the protocol draft used by client devices that associate with the access point. - Enter the name or IP address, type, port, shared secret, and timeout value for your RADIUS server. - Select the **MAC Address Authentication** checkbox under the server. **Note** You can use the same server for both EAP authentication and MAC-based authentication. On the AP Radio Advanced page (shown in Figure 4-12): - Select **Disallowed** from the pull-down menu for Default Unicast Address Filter for each authentication type requiring MAC-based authentication.
MAC-based and EAP-TLS and EAP-MD5	- Enter the settings for the EAP authentication types you need to support; select **Require EAP** on the AP Radio Data Encryption page under Open. - Enter the settings for MAC-based authentication. On the Address Filters page (shown in Figure 4-10): - Select **yes** for the setting called "Is MAC Authentication alone sufficient for a client to be fully authenticated?"
MAC-based and LEAP	- Enter the settings for LEAP. - Enter the settings for MAC-based authentication.

Setting Up Backup Authentication Servers

You can configure up to four servers for authentication services on the Authenticator Configuration page, so you can set up backup authenticators. If you set up more than one server for the same service, the server first in the list is the primary server for that service, and the other servers are used in list order when the previous server times out. If a backup server responds after the primary server fails, the access point continues to use the backup server for new transactions.

Follow these steps to set up a backup authentication server:

Step 1 Complete the steps in the "Setting Up EAP Authentication" section on page 4-19 or the "Setting Up MAC-Based Authentication" section on page 4-29 to set up your primary authentication server.

Step 2 On the Authenticator Configuration page, enter information about your backup server in one of the entry field groups under the completed entry fields for your primary server:

a. Enter the name or IP address of the backup server in the Server Name/IP entry field.

b. Enter the port number the server uses for authentication. The default setting, *1812*, is the port setting for Cisco's RADIUS server, the Cisco Secure Access Control Server (ACS), and for many other RADIUS servers. Check your server's product documentation to find the correct port setting.

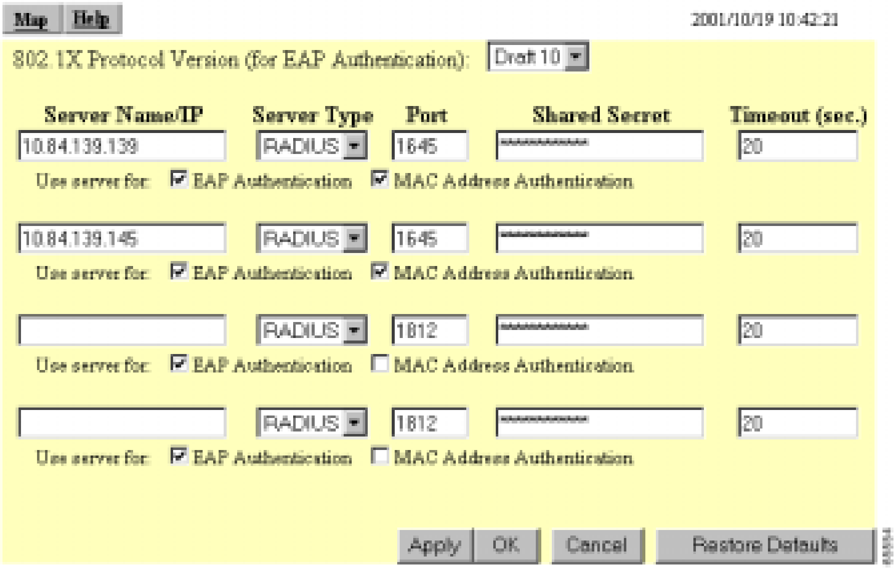
c. Enter the shared secret used by the server in the Shared Secret entry field. The shared secret on the bridge must match the shared secret on the server.

d. Enter the number of seconds the access point should try contacting the backup server in the Timeout entry field. If this backup server does not respond within this time, the access point tries to contact the next backup server on the list. If you don't have another backup server configured, the access point tries to contact the original primary authentication server.

e. Select the same authentication methods as those selected on the primary server.

Step 3 Click **OK**. You return automatically to the Setup page. Figure 4-13 shows a primary authentication server and a backup server configured on the Authenticator Configuration page.

Figure 4-13 Authenticator Configuration Page with Primary and Backup Servers



2001/10/19 10:42:21

802.1X Protocol Version (for EAP Authentication): Draft 10

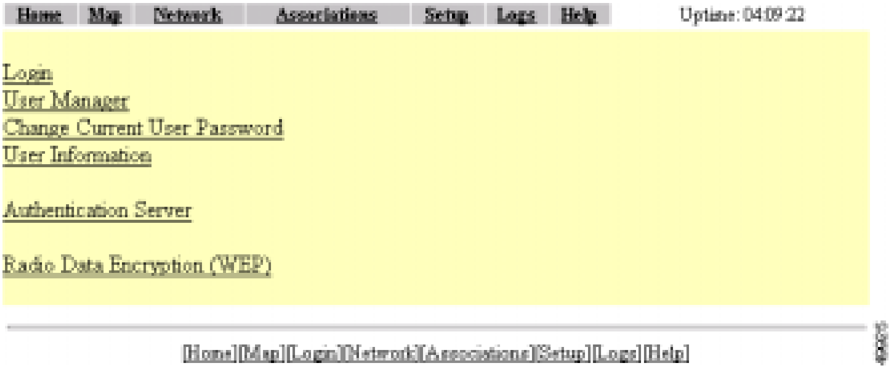
Server Name/IP	Server Type	Port	Shared Secret	Timeout (sec.)
10.84.139.139	RADIUS	1645	***********	20
Use server for:	☑ EAP Authentication	☑ MAC Address Authentication		
10.84.139.145	RADIUS	1645	***********	20
Use server for:	☑ EAP Authentication	☑ MAC Address Authentication		
	RADIUS	1812	***********	20
Use server for:	☑ EAP Authentication	☐ MAC Address Authentication		
	RADIUS	1812	***********	20
Use server for:	☑ EAP Authentication	☐ MAC Address Authentication		

Setting Up Administrator Authorization

Administrator authorization protects the access point management system from unauthorized access. Use the access point's user management pages to define a list of users who are authorized to view and change the access point management system. Use the Security Setup page to reach the user management pages. Figure 4-14 shows the Security Setup page.

Note Creating a list of users authorized to view and change the access point management system does not affect the ability of client devices to associate with the access point.

Figure 4-14 Security Setup Page


Home
Map
Network
Associations
Setup
Logs
Help
Uptime: 04:09:22
Login
User Manager
Change Current User Password
User Information
Authentication Server
Radio Data Encryption (WEP)
[Home][Map][Login][Network][Associations][Setup][Logs][Help]

Follow this link path to reach the Security Setup page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Security**.

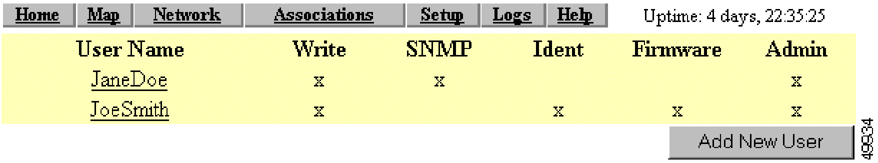
Creating a List of Authorized Management System Users

Follow these steps to create a list of users authorized to view and change the access point management system:

Step 1 Follow the link path to the Security Setup page.

Step 2 On the Security Setup page, click **User Information**. Figure 4-15 shows the User Information page.

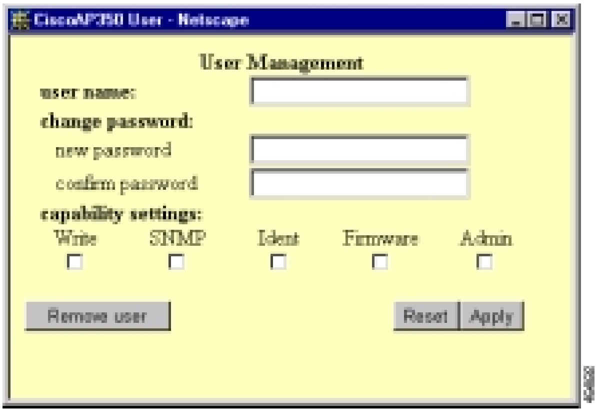
Figure 4-15 User Information Page



User Name	Write	SNMP	Ident	Firmware	Admin
JaneDoe	x	x			x
JoeSmith	x		x	x	x

Step 3 Click **Add New User**. The User Management window appears. Figure 4-16 shows the User Management window.

Figure 4-16 User Management Window



Step 4 Enter a username and password for the new user.

Step 5 Select the capabilities you want to assign to the new user. Capabilities include:

- Write—The user can change system settings. When you assign Write capability to a user, the user also automatically receives Admin capability.
- SNMP—Designates the username as an SNMP community name. SNMP management stations can use this SNMP community name to perform SNMP operations. The User Manager does not have to be enabled for SNMP communities to operate correctly.

Note Selecting the SNMP checkbox does not grant SNMP write capability to the user; it only designates the username as an SNMP community name. SNMP operations performed under the username are restricted according to the username’s other assigned capabilities.

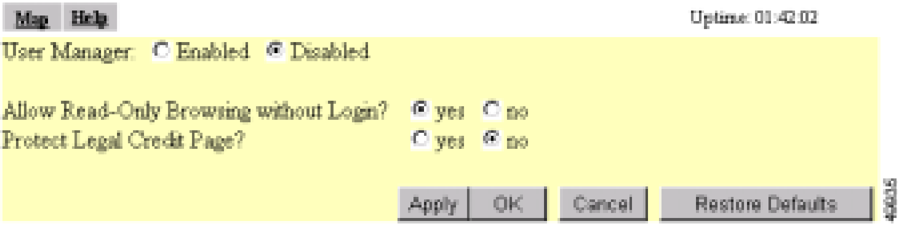
- Ident—The user can change the access point's identity settings (IP address and SSID). When you assign Ident capability to a user, the user also automatically receives Write and Admin capabilities.

- Firmware—The user can update the access point's firmware. When you assign Firmware capability to a user, the user also automatically receives Write and Admin capabilities.
- Admin—The user can view most system screens. To allow the user to view all system screens and make changes to the system, select Write capability.

Step 6 Click **Apply**. The User Management window disappears, and the new user appears in the user list on the User Information page.

Step 7 Click the browser’s **Back** button to return to the Security Setup page. On the Security Setup page, click **User Manager**. The User Manager Setup page appears. Figure 4-17 shows the User Manager Setup page.

Figure 4-17 User Manager Setup Page



User Manager: ○ Enabled ● Disabled

Allow Read-Only Browsing without Login? ● yes ○ no

Protect Legal Credit Page? ○ yes ● no

Step 8 Select **User Manager: Enabled** to restrict use of the access point management system to users in the user list.

Note You must define a full administrator user—a user with write, identity, and firmware capabilities—before you can enable the user manager.

Use the other settings on the User Manager Setup page to add more restrictions for the management system:

- Allow Read-Only Browsing without Login—Select **yes** to allow any user to view the access point’s basic screens. Select **no** to restrict access to all of the access point’s screens to only the users in the user list.

- Protect Legal Credit Page—Select **yes** to restrict access to the Legal Credits page to users in the user list. Select **no** to allow any user to view the Legal Credits page.

Step 9 Click **OK**. You return automatically to the Security Setup page.

Network Management

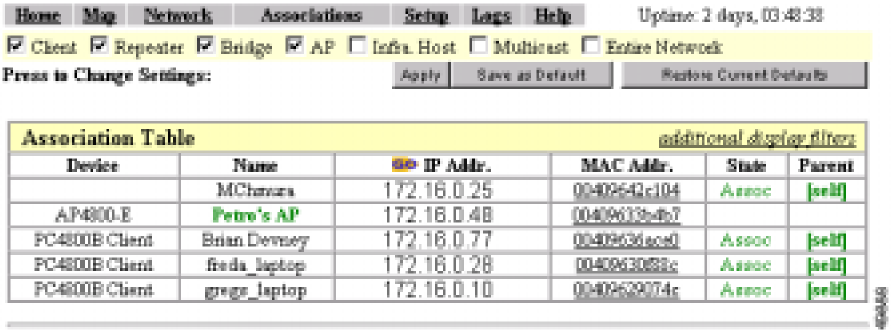
This section describes how to browse to other devices on your network, how to use Cisco Discovery Protocol with your wireless networking equipment, how to assign a specific network port to a MAC address, and how to enable wireless network accounting.

This chapter contains the following sections:

Using the Association Table

The management system's Association Table page lists all the devices, both wireless and wired to the root LAN, of which the access point is aware. Figure 5-1 shows an example of the Association Table page.

Figure 5-1 Association Table Page



Uptime: 2 days, 03:48:38

☑ Client ☑ Repeater ☑ Bridge ☑ AP □ Infra. Host □ Multicast □ Entire Network

Press to Change Settings:

Association Table

Device	Name	IP Addr.	MAC Addr.	State	Parent
	MChavara	172.16.0.25	00409642c104	Assoc	[self]
AP4800-E	Petro's AP	172.16.0.48	00409633b4b7		
PC4800B Client	Brian Devney	172.16.0.77	00409636ace0	Assoc	[self]
PC4800B Client	freda_laptop	172.16.0.28	004096308f8c	Assoc	[self]
PC4800B Client	gregs_laptop	172.16.0.10	00409629074c	Assoc	[self]

Click the **Association** link at the top of any main management system page to go to the Association Table.

Note You can also use the Association Table page in the command-line interface.

Browsing to Network Devices

To browse to a device's browser-based interface, click the device's IP address in the IP Addr. column. The home page of the device's management system appears. Cisco Aironet access points, bridges, and workgroup bridges have browser-based interfaces, and many servers and printers have them, also.

If the device does not have a browser-based interface, click the device's MAC address in the MAC Addr. column. A Station page appears for the device, displaying the information the access point knows about the device, including the device's identity and statistics on traffic to and from the device. Some devices, such as PC card client adapters, do not have browser-based interfaces.

Setting the Display Options

You use the display options to select the device types to be listed in the table. The default selections list only the access point and any devices with which it is associated. To change the selections, click a display option and then click **Apply**.

To modify the table further, click **additional display filters**, which is a link to the Association Table Filters page. You use the Association Table Filters page to select the columns of information that appear in the Association Table and the order in which devices are listed.

For more information on customizing the Association Table display, read the "Association Table Display Setup" section on page 3-62.

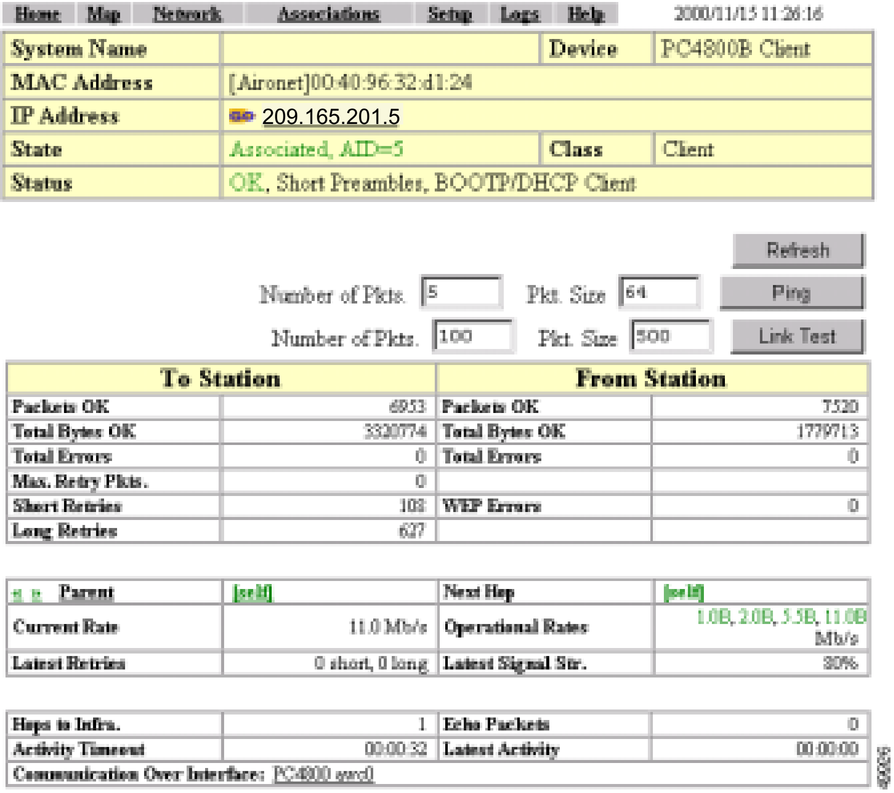
Using Station Pages

Click a device's MAC address in the Association Table's MAC Addr. column to display a Station page for the device.

Station pages provide an overview of a network device's status and data traffic history. The information on a Station page depends on the device type; a Station page for an access point, for example, contains different information than the Station page for a PC card client adapter.

You can also use the Station page to perform pings and link tests for network devices. Figure 5-2 shows a sample Station page for a PC card client adapter.

Figure 5-2 Station Page



System Name		Device	PC4800B Client
MAC Address	[Aironet]00:40:96:32:d1:24		
IP Address	209.165.201.5		
State	Associated, AID=5	Class	Client
Status	OK, Short Preambles, BOOTP/DHCP Client		

Number of Pkts. 5 Pkt. Size 64

Number of Pkts. 100 Pkt. Size 500

To Station		From Station	
Packets OK	6953	Packets OK	7520
Total Bytes OK	3320774	Total Bytes OK	1779713
Total Errors	0	Total Errors	0
Max. Retry Pkts.	0		
Short Retries	103	WEP Errors	0
Long Retries	627		

Parent	[self]	Next Hop	[self]
Current Rate	11.0 Mb/s	Operational Rates	1.0B, 2.0B, 5.5B, 11.0B Mb/s
Latest Retries	0 short, 0 long	Latest Signal Str.	30%

Hops to Infra.	1	Echo Packets	0
Activity Timeout	00:00:32	Latest Activity	00:00:00
Communication Over Interface: PC4800 awc0			

Information on Station Pages

Station Identification and Status

The yellow table at the top of the Station page lists the following information:

- System Name—The name assigned to the device.
- Device—The type and model number of the device.
- MAC Address—A unique identifier assigned by the manufacturer.
- IP Address—The device's IP address.

  When you click the IP address link, the browser attempts to display the device's home page. Cisco Aironet access points, bridges, and workgroup bridges have browser-based interfaces, and many servers and printers have them also.
- State—Displays the operational state of the wireless station. Possible states include:
  - Assoc—The station is associated with an access point. Client stations associated with this access point will also show an Association Identifier (AID) value that is an index into a table of stations associated with this access point. Maximum AID count is 2007.
  - Unauth—The station is not authenticated with any access point.
  - Auth—The station is authenticated with an access point.
  - Local Auth—The station has authenticated at least once with this access point.
- Class—This field displays the type of station. Station types include:
  - AP—An access point.
  - Client, PS Client—A client or power-save client station.
  - Bridge, Bridge R—A bridge or a root bridge.
  - Rptr—A repeater.
  - Mcast—A multicast address.
  - Infra—An infrastructure node, typically a workstation with a wired connection to the Ethernet network.

- Status—This field indicates the device’s operating status. Possible statuses include:
  - OK—The device is operating properly.
  - EAP Pending
  - EAP Autenticated
  - IP Forwarding Agent
  - BootP/DHCP Client—The device is using BOOTP or DHCP protocol
  - ARP Proxy Server
  - IP Virtual Router
  - WEP—WEP is enabled on the device.

To Station Information

Fields in the To Station column in the second table on the Station page contain the following information:

- Alert—Click this box if you want detailed packet trace information captured for the Association Table page. This option is only available to users with Administrator capability.
- Packets OK—Reports the number of good packets coming to the station.
- Total Bytes OK—Reports the number of good bytes coming to the station.
- Total Errors—Reports the total number of packet errors coming to the station.
- Max. Retry Pkts.—Reports the number of times data packets have reached the maximum long or short retry number. Set the maximum RTS value on the AP Radio Hardware page; see the “Entering Radio Hardware Information” section on page 3-21 for instructions.
- RTS (Short) Retries—Reports the number of times the RTS packet had to be retried.
- Data (Long) Retries—Reports the number of times the data packet had to be retried.

From Station Information

Fields in the To Station column contain the following information:

- Alert—Click this box if you want detailed packet trace information captured for the Association Table page. This option is only available to users with Administrator capability.
- Packets OK—Reports the number of good packets sent from the station.
- Total Bytes OK—Reports the number of good bytes sent from the station.
- Total Errors—Reports the total number of packet errors sent from the station.
- WEP Errors—Reports the number of encryption errors sent from the station.

Rate, Signal, and Status Information

The table under the To and From Station table lists rate, signal, and status information for the device.

Data rate and signal quality information appears on Station pages for client devices. On Station pages for access points, this area shows network information such as system uptime.

- Parent—Displays the system name of the device to which the client, bridge or repeater is associated. The entry [self] indicates that the device is associated with this access point.
- Current Rate—Reports the current data transmission rate. If the station is having difficulty communicating with the access point, this might not be the highest operational rate.
- Latest Retries—Tally of short and long data retries.
- Next Hop—If repeater access points are used on the network, this field names the next access point in the repeater chain.
- Operational Rates—The data transmission rates in common between the access point and the station.
- Latest Signal Strength—Displays the current index of radio signal quality.

The following four fields appear only on the Station page for an access point:

- Stations Associated—Displays, by number and class, all stations associated with the access point.

- Uptime—Displays the cumulative time the device has been operating since the last reset.
- Software Version—Displays the version level of Cisco software on the device.
- Announcement Packets—Total number of Announcement packets since the device was last reset.

Hops and Timing Information

The table at the bottom of the Station page lists information on the chain of devices, if any, between the device and the wired LAN, on the monitoring timeout for the device, and on the time of the most recent system activity.

- Hops to Infra.—The number of devices between this station and the network infrastructure.
- Activity Timeout—Total time that can elapse after the access point's last data receipt before the access point presumes the client device has been turned off. See the "Association Table Advanced Page" section on page 3-66 for information on setting timeouts for each device class.
- Communication Over Interface—The network port over which the access point or bridge is communicating with the device.
- Echo Packets—The link test sequence number; it lists the total number of link test packets sent to this station.
- Latest Activity—Elapsed time in hours, minutes, and seconds since the station and the access point last communicated. All zeros means there is current communication.

Performing Pings and Link Tests

Use the ping and link test buttons to perform pings and link tests on the device. If the device is associated to the access point through which you reached the Station page, the link test button and packet fields appear. If the device is not associated with the access point, only the ping button and packet fields appear.

Performing a Ping

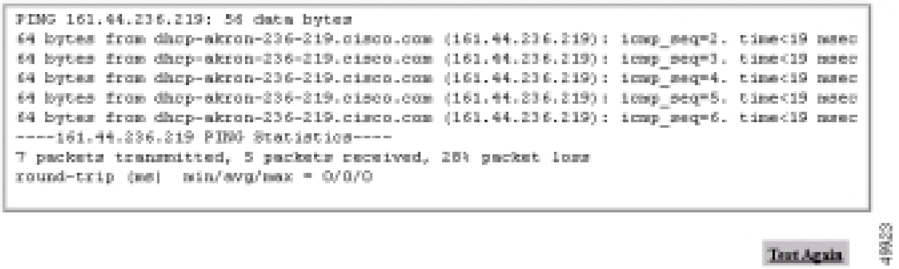
Follow these steps to ping the device described on the Station page:

Step 1 To customize the size and number of packets sent during the ping, enter the number of packets and size of the packets in the Number of Pkts. and Pkt. Size fields.

Step 2 Click **Ping**.

The ping runs using the values in the Number of Pkts. and Pkt. Size fields, and a ping window appears listing the test results. To run the ping again, click **Test Again**. Figure 5-3 shows a ping window.

Figure 5-3 Ping Window



```
PING 161.44.236.219: 56 data bytes
64 bytes from dhcp-akron-236-219.cisco.com (161.44.236.219): icmp_seq=2. time<19 msec
64 bytes from dhcp-akron-236-219.cisco.com (161.44.236.219): icmp_seq=3. time<19 msec
64 bytes from dhcp-akron-236-219.cisco.com (161.44.236.219): icmp_seq=4. time<19 msec
64 bytes from dhcp-akron-236-219.cisco.com (161.44.236.219): icmp_seq=5. time<19 msec
64 bytes from dhcp-akron-236-219.cisco.com (161.44.236.219): icmp_seq=6. time<19 msec
----161.44.236.219 PING Statistics----
7 packets transmitted, 5 packets received, 28% packet loss
round-trip (ms)  min/avg/max = 0/0/0
```

Performing a Link Test

Follow these steps to perform a link test between the access point and the device described on the Station page:

Step 1 To customize the size and number of packets sent during the link test, enter the number of packets and size of the packets in the Number of Pkts. and Pkt. Size fields.

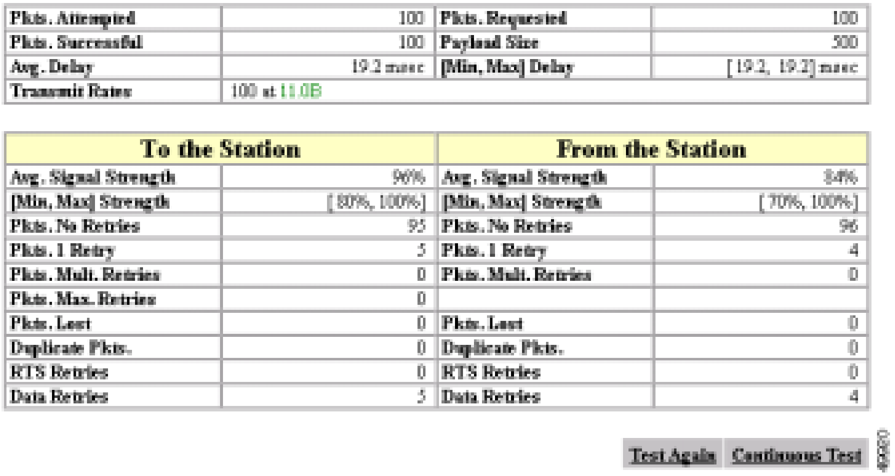
Step 2 Click **Link Test**.

The link test runs using the values in the Number of Pkts. and Pkt. Size fields.

Note If you need to stop the link test before the test is complete, click **Stop Test**.

A results window appears listing the test results. To run the test again, click **Test Again**. To run a continuous link test, click **Continuous Test**. Figure 5-4 shows a link test results window.

Figure 5-4 Link Test Results Window



Pkts. Attempted	100	Pkts. Requested	100
Pkts. Successful	100	Payload Size	500
Avg. Delay	19.2 msec	[Min, Max] Delay	[19.2, 19.2] msec
Transmit Rates	100 at 11.0B		

To the Station		From the Station	
Avg. Signal Strength	96%	Avg. Signal Strength	84%
[Min, Max] Strength	[80%, 100%]	[Min, Max] Strength	[70%, 100%]
Pkts. No Retries	95	Pkts. No Retries	96
Pkts. 1 Retry	5	Pkts. 1 Retry	4
Pkts. Mult. Retries	0	Pkts. Mult. Retries	0
Pkts. Max. Retries	0		
Pkts. Lost	0	Pkts. Lost	0
Duplicate Pkts.	0	Duplicate Pkts.	0
RTS Retries	0	RTS Retries	0
Data Retries	5	Data Retries	4

Clearing and Updating Statistics

Use the Clear Stats and Refresh buttons to clear and update the Station page statistics.

- Clear Stats—Clears all packet, octet and error counts and resets the counters to 0.
- Refresh—Updates the counts to their latest accumulated values, and saves the Alert selections.

Deauthenticating and Disassociating Client Devices

Use the Deauthenticate and Disassociate buttons to deauthenticate and disassociate the client device from the access point. These buttons appear only on Station pages for devices that are associated with the access point, and only users with administrator capability can operate them.

- Deauthenticate—Forces a client to re-authenticate with the access point.
- Disassociate—Allows a client to break its current association, re-evaluate the currently associated access point and determine which of the surrounding access points has the best signal quality to associate with.

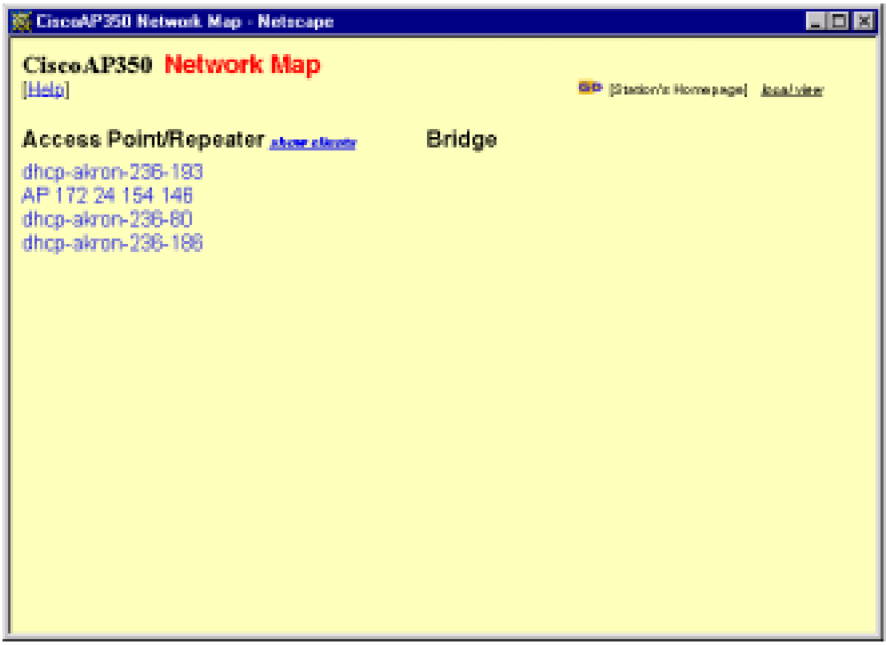
Using the Network Map Window

To open the Network Map window, click **Map** at the top of any management system page. (See the “Navigating Using the Map Windows” section on page 2-4 for information about the Map page.) When the Map window appears, click **Network Map**.

You use the Network Map window to open a new browser window displaying information for any device on your wireless network. Unlike the Association Table, the Network Map window does not list wired devices on your LAN. Figure 5-5 shows the Network Map window.

Note Your Internet browser must have Java enabled to use the map windows.

Figure 5-5 Network Map Window



CiscoAP350 Network Map
[Help]

[Station's Homepage] local view

Access Point/Repeater show clients

Bridge

dhcp-akron-236-193
AP 172 24 154 146
dhcp-akron-236-80
dhcp-akron-236-188

Click the name of a wireless device to open a new browser window displaying a Station page displaying the access point's local information for that device. Click **Go** beside the device name to open a new browser window displaying that device's home page, if available. Some devices, such as PC card clients, do not have browser-based interfaces.

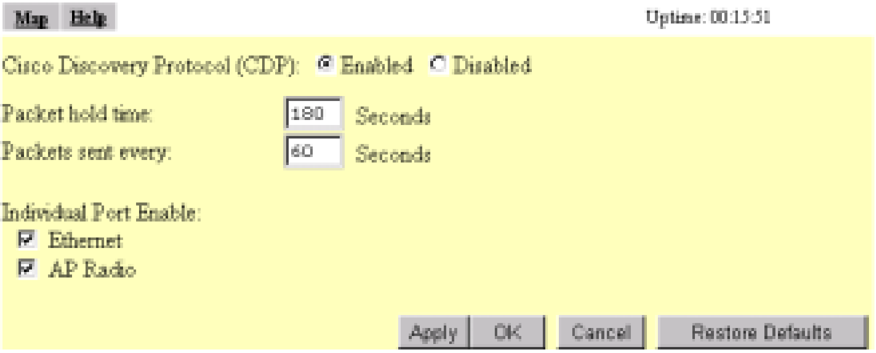
Click **show clients** to display all the wireless client devices on your network. The client names appear under the access point or bridge with which they are associated. If clients are displayed, click **hide clients** to display only non-client devices.

Using Cisco Discovery Protocol

Cisco Discovery Protocol (CDP) is a device-discovery protocol that runs on all Cisco network equipment. Each device sends identifying messages to a multicast address, and each device monitors the messages sent by other devices. Information in CDP packets is used in network management software such as CiscoWorks2000.

Use the CDP Setup page to adjust the access point's CDP settings. CDP is enabled by default. Figure 5-6 shows the CDP Setup page.

Figure 5-6 CDP Setup Page



Uptime: 00:15:51

Cisco Discovery Protocol (CDP): ● Enabled ○ Disabled

Packet hold time: 180 Seconds

Packets sent every: 60 Seconds

Individual Port Enable:

☑ Ethernet

☑ AP Radio

Follow this link path to reach the CDP Setup page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Cisco Services**.
3. On the Cisco Services Setup page, click **Cisco Discovery Protocol (CDP)**.

Settings on the CDP Setup Page

The CDP Setup page contains the following settings:

- Enabled/Disabled—Select **Disabled** to disable CDP on the access point; select **Enabled** to enable CDP on the access point. CDP is enabled by default.
- Packet hold time—The number of seconds other CDP-enabled devices should consider the access point’s CDP information valid. If other devices do not receive another CDP packet from the access point before this time elapses they should assume that the access point has gone offline. The default value is 180. The packet hold time should always be greater than the value in the “Packets sent every” field.
- Packets sent every—The number of seconds between each CDP packet the access point sends. The default value is 60. This value should always be less than the packet hold time.
- Individual Port Enable: Ethernet—When selected, the access point sends CDP packets through its Ethernet port and monitors the Ethernet for CDP packets from other devices.
- Individual Port Enable: AP Radio—This checkbox appears when the access point radio is linked to another radio infrastructure device, such as an access point or a bridge. When selected, the access point sends CDP packets through the radio port and monitors the radio for CDP packets from other devices.

MIB for CDP

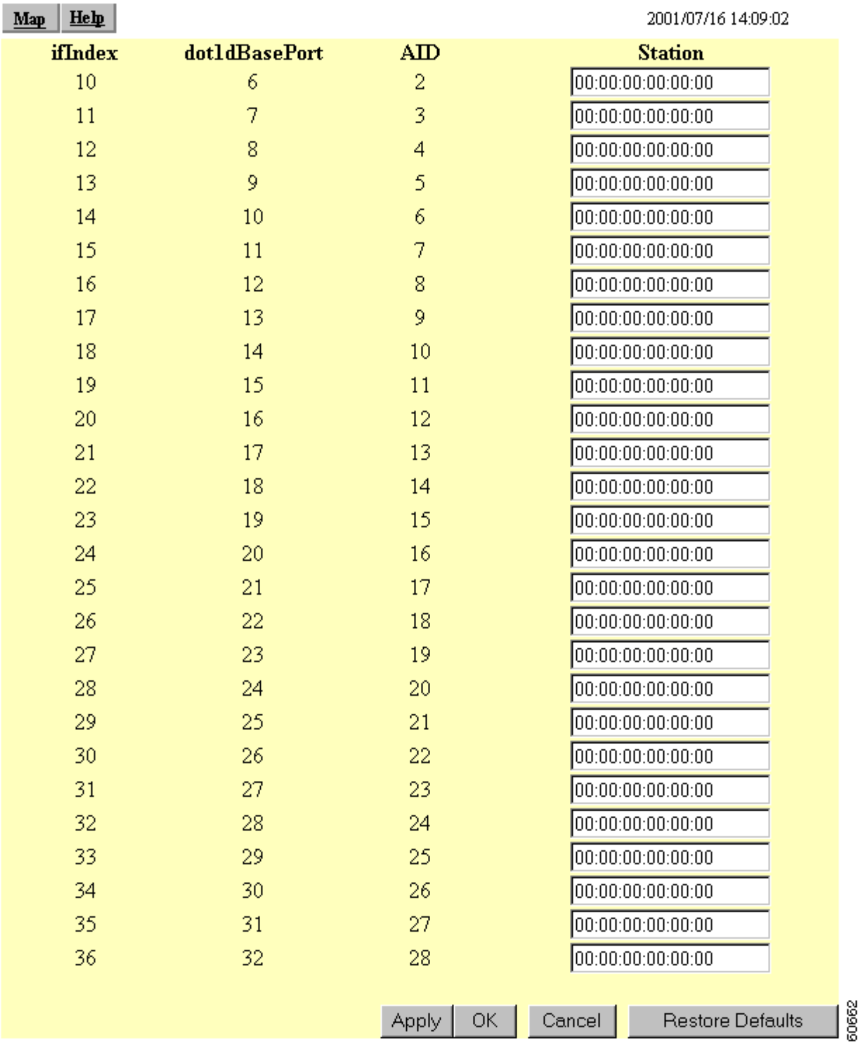
A MIB file is available for use with CDP. The filename is CISCO-CDP-MIB.my, and you can download the MIB at the following URL:

http://www.cisco.com/public/mibs

Assigning Network Ports

Use the Port Assignments page to assign a specific network port to a repeater access point or to a non-root bridge. When you assign specific ports, your network topology remains constant even when devices reboot. Figure 5-7 shows the Port Assignments page.

Figure 5-7 Port Assignments Page



2001/07/16 14:09:02

ifIndex	dot1dBasePort	AID	Station
10	6	2	00:00:00:00:00:00
11	7	3	00:00:00:00:00:00
12	8	4	00:00:00:00:00:00
13	9	5	00:00:00:00:00:00
14	10	6	00:00:00:00:00:00
15	11	7	00:00:00:00:00:00
16	12	8	00:00:00:00:00:00
17	13	9	00:00:00:00:00:00
18	14	10	00:00:00:00:00:00
19	15	11	00:00:00:00:00:00
20	16	12	00:00:00:00:00:00
21	17	13	00:00:00:00:00:00
22	18	14	00:00:00:00:00:00
23	19	15	00:00:00:00:00:00
24	20	16	00:00:00:00:00:00
25	21	17	00:00:00:00:00:00
26	22	18	00:00:00:00:00:00
27	23	19	00:00:00:00:00:00
28	24	20	00:00:00:00:00:00
29	25	21	00:00:00:00:00:00
30	26	22	00:00:00:00:00:00
31	27	23	00:00:00:00:00:00
32	28	24	00:00:00:00:00:00
33	29	25	00:00:00:00:00:00
34	30	26	00:00:00:00:00:00
35	31	27	00:00:00:00:00:00
36	32	28	00:00:00:00:00:00

Follow this link path to reach the Port Assignments page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Port Assignments** in the Association section near the top of the page.

Settings on the Port Assignments Page

- ifIndex—Lists the port's designator in the Standard MIB-II (RFC1213-MIB.my) interface index.
- dot1dBasePort—Lists the port's designator in the Bridge MIB (RFC1493; BRIDGE-MIB.my) interface index.
- AID—Lists the port's 802.11 radio drivers association identifier.
- Station—Enter the MAC address of the device to which you want to assign the port in the port's Station entry field. When you click **Apply** or **OK**, the port is reserved for that MAC address.

Enabling Wireless Network Accounting

You can enable accounting on the access point to send network accounting information about wireless client devices to a RADIUS server on your network. Cisco Secure ACS writes accounting records to a log file or to a database daily. Consult the *Cisco Secure ACS 2.6 for Windows 2000/NT Servers User Guide* for instructions on viewing and downloading the log or database:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/csnt26/index.htm

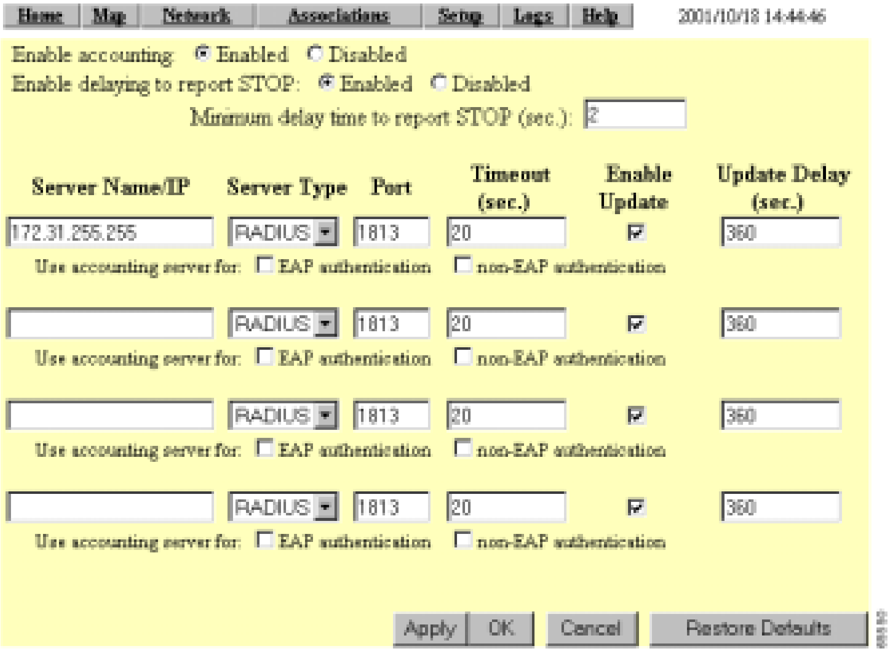
If you have a UNIX server, use this URL to browse to the *CiscoSecure ACS 2.3 for UNIX User Guide*:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/cs_unx/csu23ug/index.htm

Note RADIUS accounting is available in firmware versions 11.10T and later, which are available on Cisco.com. You can download Cisco Aironet firmware releases at http://www.cisco.com/public/sw-center/sw-wireless.shtml.

Use the Accounting Setup page to enable and set up accounting on the access point. Figure 5-8 shows the Accounting Setup page.

Figure 5-8 Accounting Setup Page



Enable accounting: ● Enabled ○ Disabled
Enable delaying to report STOP: ● Enabled ○ Disabled
Minimum delay time to report STOP (sec.): 2

Server Name/IP	Server Type	Port	Timeout (sec.)	Enable Update	Update Delay (sec.)
172.31.255.255	RADIUS	1813	20	☑	360
Use accounting server for:	□ EAP authentication		□ non-EAP authentication		
	RADIUS	1813	20	☑	360
Use accounting server for:	□ EAP authentication		□ non-EAP authentication		
	RADIUS	1813	20	☑	360
Use accounting server for:	□ EAP authentication		□ non-EAP authentication		
	RADIUS	1813	20	☑	360
Use accounting server for:	□ EAP authentication		□ non-EAP authentication		

Follow this link path to reach the Accounting Setup page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Accounting** under Services.

Settings on the Accounting Setup Page

The Accounting Setup page contains these settings:

- Enable accounting—Select Enabled to turn on accounting for your wireless network.
- Enable delaying to report stop—Select this option to delay sending a stop report to the server when a client device disassociates from the access point. The delay reduces accounting activity for client devices that disassociate from the access point and then quickly reassociate.

- Minimum delay time to report stop (sec.)—Enter the number of seconds the access point waits before sending a stop report to the server when a client device disassociates from the access point. The delay reduces accounting activity for client devices that disassociate from the access point and then quickly reassociate.
- Server Name/IP—Enter the name or IP address of the server to which the access point sends accounting data.
- Server Type—Select the server type from the pull-down menu. RADIUS is the only menu option; additional types will be added in future software releases.
- Port—The communication port setting used by the access point and the server. The default setting, 1813, is the correct setting for Cisco Aironet access points and Cisco secure ACS.
- Timeout (sec.)—Enter the number of seconds the access point should wait before giving up contacting the server. If the server does not respond within this time, the access point tries to contact the next accounting server in the list if one is specified. The access point uses backup servers in list order when the previous server times out.
- Enable Update—Click the Enable Update checkbox to enable accounting update messages for wireless clients. With updates enabled, the access point sends an accounting start message when a wireless client associates to the access point, sends updates at regular intervals while the wireless client is associated to the access point, and sends an accounting stop message when the client disassociates from the access point. With updates disabled, the access point sends only accounting start and accounting stop messages to the server.
- Update Delay—Enter the update interval in seconds. If you use 360, the default setting, the access point sends an accounting update message for each associated client device every 6 minutes.
- Use accounting server for—Select the authentication types for which you want to collect accounting data. When you select **EAP authentication**, the access point sends accounting data to the server for client devices that authenticate using Cisco Aironet LEAP, EAP-TLS, or EAP-MD5. When you select **non-EAP authentication**, the access point sends data to the server for client devices using authentication types other than EAP, such as open, shared key, or MAC-based authentication.

Accounting Attributes

Table 5-1 lists the accounting attributes the access point sends to the accounting server.

Table 5-1 Accounting Attributes the Access Point Sends to the Accounting Server

Attribute	Definition
Acct-Status-Type	The client device's current accounting status; possible statuses include ACCT_START, ACCT_STOP, and ACCT_UPDATE. The access point sends an ACCT_START frame to the accounting server when a client device successfully authenticates on a RADIUS server through the access point; the access point sends an ACCT_STOP frame to the server when a client device disassociates from the access point; and the access point sends an ACCT_UPDATE frame to the server periodically while the authenticated client device is associated to the access point.
Acct-Session-ID	A unique accounting identifier for each connection activity that is bounded by ACCT_START and ACCT_STOP. The access point sends this attribute to the server with all three status types.
User-Name	The username with which the client device's authenticated to the network. The access point sends this attribute to the server with all three status types.
NAS-Port	The port number used for the client device's connection. The access point sends this attribute to the server with all three status types.
Acct-Authentic	The method with which the client device is authenticated to the network. This value is always 1, which represents RADIUS authentication. The access point sends this attribute to the server with all three status types.

Table 5-1 Accounting Attributes the Access Point Sends to the Accounting Server (continued)

Attribute	Definition
NAS-Identifier	The network access server (NAS) sending the accounting data; for wireless networks, the name of the access point sending the accounting information. The access point sends this attribute to the server with all three status types.
Acct-Session-Time	The elapsed time in seconds that the client device has been associated to the access point. The access point sends this attribute only with the ACCT_STOP and ACCT_UPDATE status types.
Acct-Input-Octets	The number of octets received on the wireless network through the access point since the client device associated to the access point. The access point sends this attribute only with the ACCT_STOP and ACCT_UPDATE status types.
Acct-Output-Octets	The number of octets sent on the wireless network through the access point since the client device associated to the access point. The access point sends this attribute only with the ACCT_STOP and ACCT_UPDATE status types.
Acct-Input-Packets	The number of packets received on the wireless network through the access point since the client device associated to the access point. The access point sends this attribute only with the ACCT_STOP and ACCT_UPDATE status types.
Acct-Output-Packets	The number of packets sent on the wireless network through the access point since the client device associated to the access point. The access point sends this attribute only with the ACCT_STOP and ACCT_UPDATE status types.
Acct-Terminate-Cause	How the client device’s session was terminated. This attribute lists the same cause for every disassociated client device: Loss of service. The access point sends this attribute only with the ACCT_STOP status type.

Table 5-1 Accounting Attributes the Access Point Sends to the Accounting Server (continued)

Attribute	Definition
Acct-Delay-Time	The delay between the time the event occurred and the time that the attribute was sent to the server. The access point sends this attribute to the server with all three status types.
RADIUS_IPADR	The IP address of the access point sending the accounting information. The access point sends this attribute to the server with all three status types.

Managing Firmware and Configurations

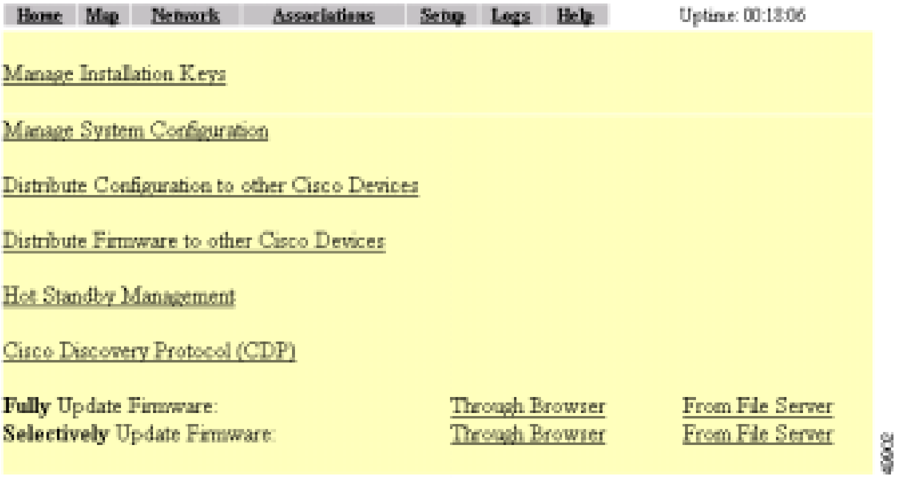
This section describes how to update the firmware version on the access point, how to distribute firmware to other access points, how to distribute the access point's configuration to other access points, and how to download, upload, and reset the access point configuration. You use the Cisco Services Setup page as a starting point for all these activities.

This chapter contains the following sections:

Updating Firmware

You use the Cisco Services Setup page to update the access point's firmware. You can perform the update by browsing to a local drive or by using FTP to update the firmware from a file server. Figure 6-1 shows the Cisco Services Setup page.

Figure 6-1 Cisco Services Setup Page



Manage Installation Keys

Manage System Configuration

Distribute Configuration to other Cisco Devices

Distribute Firmware to other Cisco Devices

Hot Standby Management

Cisco Discovery Protocol (CDP)

Fully Update Firmware: Through Browser From File Server
Selectively Update Firmware: Through Browser From File Server

Follow this link path in the browser interface to reach the Cisco Services Setup page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Cisco Services Setup**.

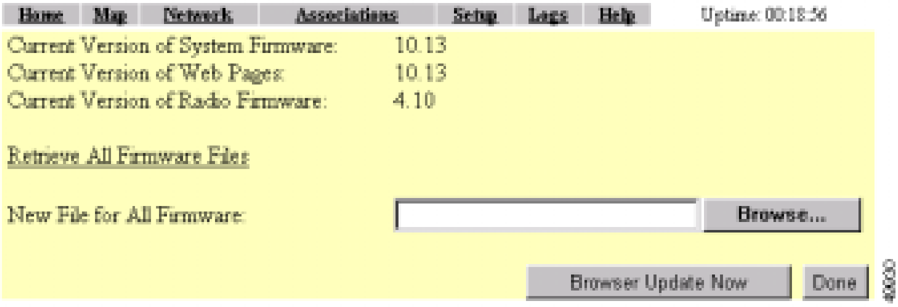
Updating with the Browser from a Local Drive

When you update the firmware with your browser, you browse to your hard drive or to a mapped network drive for the new firmware. You can update the three firmware components—the management system firmware, the firmware web pages, and the radio firmware—individually or all at once. It is simplest to update all the components at once, but in some situations you might want to update them individually.

Full Update of the Firmware Components

To update all the firmware components at the same time, click **Through Browser** on the Fully Update Firmware line on the Cisco Services Setup page. The Update All Firmware Through Browser page appears. Figure 6-2 shows the Update All Firmware Through Browser page.

Figure 6-2 Update All Firmware Through Browser Page



Uptime: 00:18:56

Current Version of System Firmware: 10.13
Current Version of Web Pages: 10.13
Current Version of Radio Firmware: 4.10

Retrieve All Firmware Files

New File for All Firmware:

Follow these steps to update all three firmware components through the browser:

Step 1 If you know the exact path and filename of the new firmware image file, type it in the New File for All Firmware entry field.

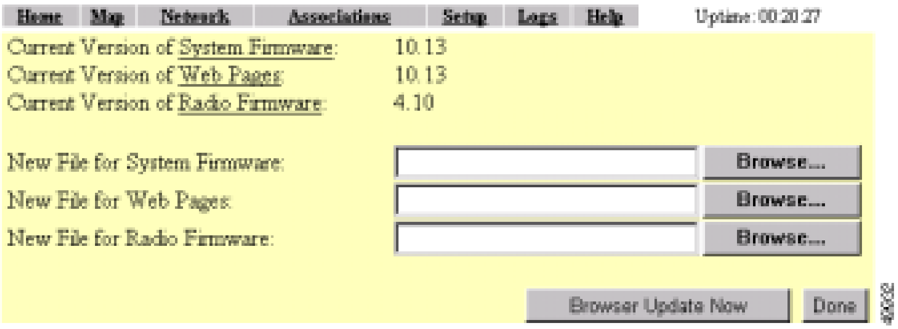
If you aren’t sure of the exact path to the new firmware image file, click **Browse...** next to the New File entry field. When the File Upload window appears, go to the directory that contains the firmware image file and select the file. Click **Open**.

Step 2 When the filename for the new firmware appears in the New File entry field, click **Browser Update Now** to load and install the new firmware. When the update is complete, the access point automatically reboots.

Selective Update of the Firmware Components

To update firmware components individually, click **Through Browser** on the Selectively Update Firmware line on the Cisco Services Setup page. The Update Firmware Through Browser page appears. Figure 6-3 shows the Update Firmware Through Browser page.

Figure 6-3 Update Firmware Through Browser Page



Current Version of System Firmware: 10.13
Current Version of Web Pages: 10.13
Current Version of Radio Firmware: 4.10

New File for System Firmware:
New File for Web Pages:
New File for Radio Firmware:

Follow these steps to update one of the three firmware components through the browser:

Step 1 If you know the exact path and filename of the new firmware component, type it in the New File for [component] entry field.

If you aren't sure of the exact path to the new component, click **Browse...** next to the component's New File entry field. When the File Upload window appears, go to the directory that contains the component and select the file. Click **Open**.

Step 2 When the filename for the new component appears in the New File entry field, click **Browser Update Now** to load and install the new component. When the update is complete, the AP automatically reboots.

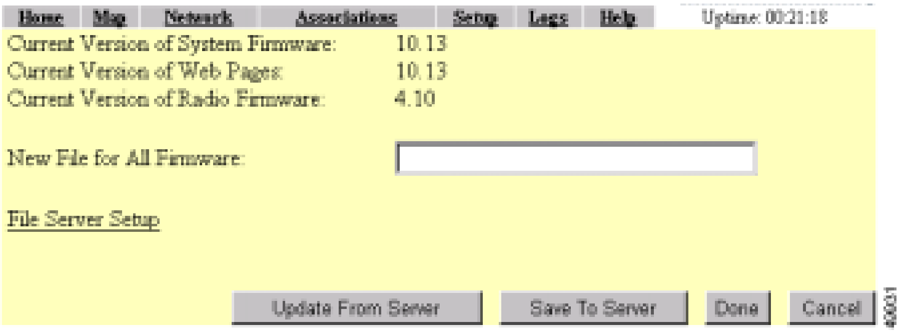
Updating from a File Server

When you update the firmware from a file server, you load new firmware through FTP or TFTP from a file server. You can update the three firmware components—the management system firmware, the firmware web pages, and the radio firmware—individually or all at once. It is simplest to update all the components at once, but in some situations you might want to update them individually.

Full Update of the Firmware Components

To update all the firmware components at the same time, click **From File Server** on the Fully Update Firmware line on the Cisco Services Setup page. The Update All Firmware From File Server page appears. Figure 6-4 shows the Update All Firmware From File Server page.

Figure 6-4 Update All Firmware From File Server Page



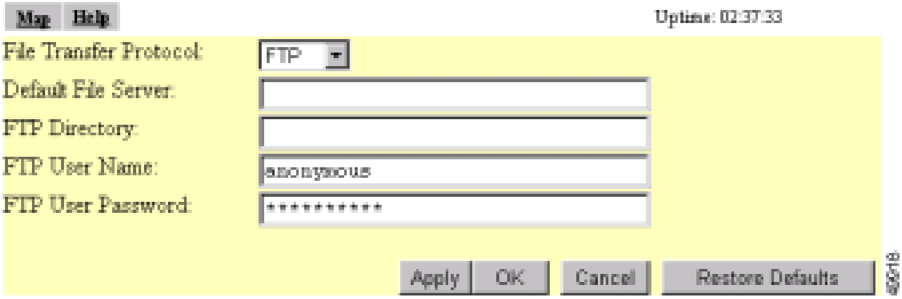
Current Version of System Firmware: 10.13
Current Version of Web Pages: 10.13
Current Version of Radio Firmware: 4.10

New File for All Firmware:

Follow these steps to update all three firmware components from a file server:

Step 1 Click the File Server Setup link to enter the FTP settings. The FTP Setup page appears. Figure 6-5 shows the FTP Setup page.

Figure 6-5 FTP Setup Page



File Transfer Protocol: FTP

Default File Server:

FTP Directory:

FTP User Name: anonymous

FTP User Password: **********

Step 2 Enter the FTP settings on the FTP Setup page.

- **a.** Select FTP or TFTP from the File Transfer Protocol pull-down menu. FTP (File Transfer Protocol) is the standard protocol that supports transfers of data between local and remote computers. TFTP (Trivial File Transfer Protocol) is a relatively slow, low-security protocol that requires no user name or password.
- **b.** In the Default File Server entry field, enter the IP address of the server where the access point should look for FTP files.
- **c.** In the FTP Directory entry field, enter the directory on the server where FTP files are located.
- **d.** In the FTP User Name entry field, enter the user name assigned to the FTP server. If you selected TFTP, you can leave this field blank.
- **e.** In the FTP Password entry field, enter the password associated with the user name. If you selected TFTP, you can leave this field blank.
- **f.** Click **OK**. You return automatically to the Update All Firmware Through File Server page.

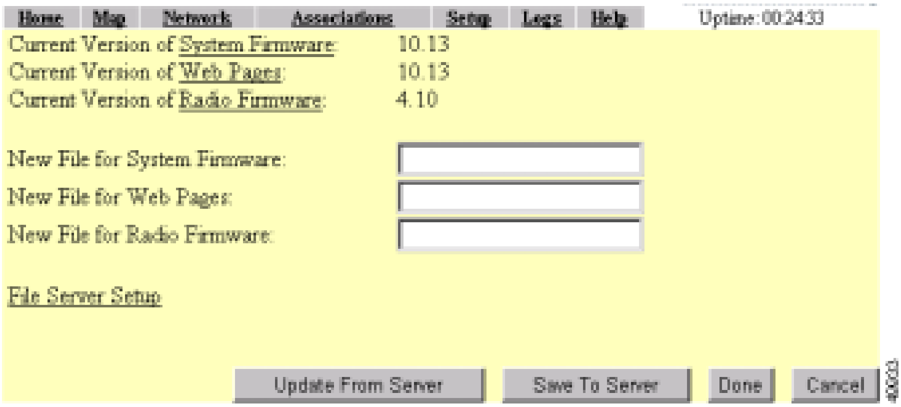
Step 3 On the Update All Firmware Through File Server page, type the filename of the new firmware image file in the New File for All Firmware entry field.

Step 4 Click **Browser Update Now** to load and install the new firmware. When the update is complete, the access point automatically reboots.

Selective Update of the Firmware Components

To update firmware components individually, click **From File Server** on the Selectively Update Firmware line on the Cisco Services Setup page. The Update Firmware From File Server page appears. Figure 6-6 shows the Update Firmware From File Server page.

Figure 6-6 Update Firmware From File Server Page



Current Version of System Firmware: 10.13
Current Version of Web Pages: 10.13
Current Version of Radio Firmware: 4.10

New File for System Firmware:
New File for Web Pages:
New File for Radio Firmware:

File Server Setup

To update one of the three firmware components from the file server, follow the steps listed in the "Full Update of the Firmware Components" section on page 6-5, but in Step 3, type the filenames of the firmware components you want to update in the components' entry fields. Click **Browser Update Now** to load and install the new firmware. When the update is complete, the access point automatically reboots.

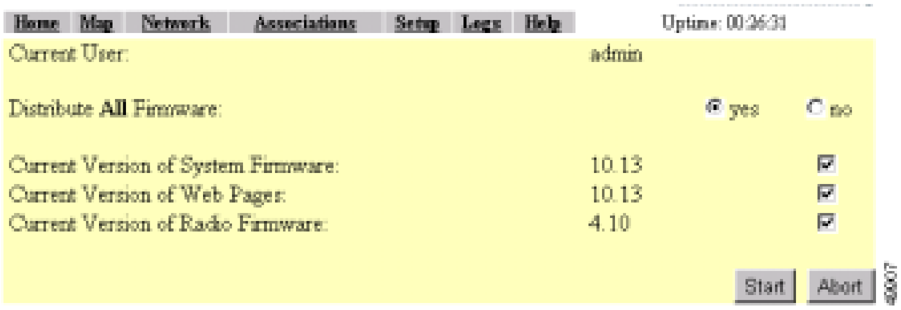
Distributing Firmware

You use the Distribute Firmware page to distribute the access point's firmware to other Cisco Aironet access points. Figure 6-7 shows the Distribute Firmware page.

The access point sends its firmware to all the access points on your network that:

- Are running access point firmware version 10.00 or newer
- Can detect the IP multicast query issued by the distributing access point (network devices such as routers can block multicast messages)
- Have their web servers enabled for external browsing (see the "Entering Web Server Settings and Setting Up Access Point Help" section on page 3-53)
- Have the same HTTP port setting as the distributing access point (the HTTP port setting is on the Web Server Setup page)
- Have a Default Gateway setting other than the default setting, which is 255.255.255.255 (the Default Gateway setting is on the Express Setup and Routing Setup pages)
- If they have User Manager enabled, contain in their User Lists a user with the same user name, password, and capabilities as the user performing the distribution (the person logged in on the distributing access point)

Figure 6-7 Distribute Firmware Page



Uptime: 00:26:31

Current User: admin

Distribute All Firmware: ● yes ○ no

Current Version of System Firmware: 10.13 ☑
Current Version of Web Pages: 10.13 ☑
Current Version of Radio Firmware: 4.10 ☑

Follow this link path in the browser interface to reach the Distribute Firmware page:

1. On the Summary Status page, click **Setup**.

2. On the Setup page, click **Cisco Services Setup**.
3. On the Cisco Services page, click **Distribute Firmware to other Cisco Devices**.

Follow these steps to distribute firmware to other access points:

Step 1 Follow the link path to reach the Distribute Firmware page.

Step 2 To distribute all three firmware components at once, verify that *yes* is selected for Distribute All Firmware. This is the default setup for the Distribute Firmware page.

To distribute the firmware components individually, select **no** for Distribute All Firmware, and click the checkboxes for the components you want to distribute.

Step 3 Click **Start**. The access point's firmware is distributed to the access points on your network. To cancel the distribution, click **Abort**.

When the distribution is complete, the access points that received the firmware automatically reboot.

Distributing a Configuration

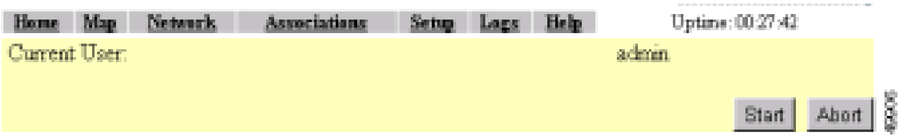
You use the Distribute Configuration page to distribute the access point's configuration to other Cisco Aironet access points. Figure 6-8 shows the Distribute Configuration page.

The access point sends its entire system configuration except for its IP identity information and its User List. The configuration is sent and applied to all the access points on your network that:

- Are running access point firmware version 10.05 or newer
- Can detect the IP multicast query issued by the distributing access point (network devices such as routers can block multicast messages)
- Have their web servers enabled for external browsing (see the "Entering Web Server Settings and Setting Up Access Point Help" section on page 3-53)
- Have the same HTTP port setting as the distributing access point (the HTTP port setting is on the Web Server Setup page)

- Have a Default Gateway setting other than the default setting, which is 255.255.255.255 (the Default Gateway setting is on the Express Setup and Routing Setup pages)
- If they have User Manager enabled, contain in their User Lists a user with the same user name, password, and capabilities as the user performing the distribution (the person logged in on the distributing access point)

Figure 6-8 Distribute Configuration Page



Uptime: 00:27:42

Current User: admin

Follow this link path in the browser interface to reach the Distribute Configuration page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Cisco Services Setup**.
3. On the Cisco Services page, click **Distribute Configuration to other Cisco Devices**.

Follow these steps to distribute the access point's configuration to other access points:

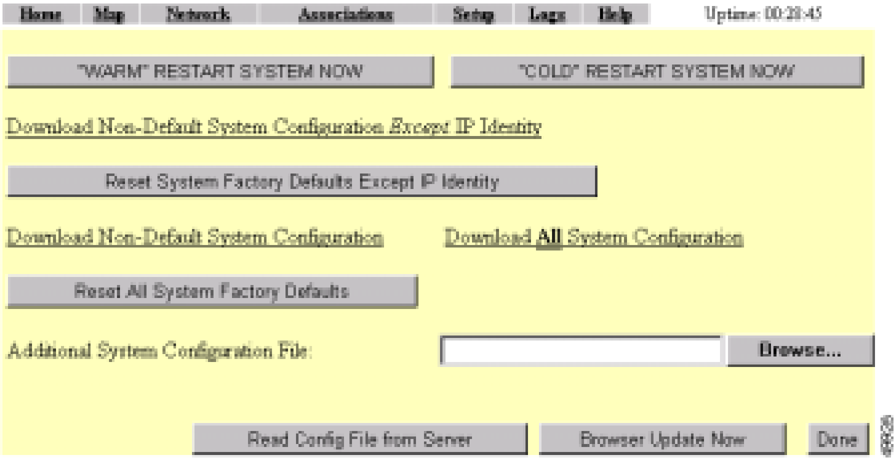
Step 1 Follow the link path to reach the Distribute Configuration page.

Step 2 Click **Start**. The access point's configuration, except for its IP identity and its User List, is distributed to the access points on your network. To cancel the distribution, click **Abort**.

Downloading, Uploading, and Resetting the Configuration

You use the System Configuration Setup page to download the current access point configuration to a local drive, upload a configuration from a local drive or file server, and reset the configuration to default settings. You can also use the System Configuration Setup page to restart the access point. Figure 6-9 shows the System Configuration Setup page.

Figure 6-9 System Configuration Setup Page


Home
Map
Network
Associations
Setup
Logs
Help
Uptime: 00:20:45
"WARM" RESTART SYSTEM NOW
"COLD" RESTART SYSTEM NOW
Download Non-Default System Configuration Except IP Identity
Reset System Factory Defaults Except IP Identity
Download Non-Default System Configuration
Download All System Configuration
Reset All System Factory Defaults
Additional System Configuration File:
Browse...
Read Config File from Server
Browser Update Now
Done

Follow this link path in the browser interface to reach the System Configuration Setup page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Cisco Services Setup**.
3. On the Cisco Services page, click **Manage System Configuration**.

Downloading the Current Configuration

Follow these steps to download the access point's current configuration to your hard drive or to a mapped network drive:

Step 1 Follow the link path to the System Configuration Setup page.

Step 2 If your web browser is Microsoft Windows Internet Explorer, use the download configuration links to save the configuration file:

- Click **Download System Configuration Except IP Identity** to save an .ini file containing the current configuration except for the access point's IP address.
- To save the current non-default configuration including the access point's IP address, click **Download Non-Default System Configuration**.
- To save the current default and non-default configuration including the access point's IP address, click **Download All System Configuration**.

If your web browser is Netscape Communicator, use your right mouse button to click the download configuration links and select **Save link as** in the pop-up menu. If you click the links with your left mouse button, Netscape Communicator displays the text file but does not open the Save as window.

Step 3 When the Save as window appears, select the drive and directory where you want to save the file, and provide a filename for the configuration file. Click **Save**.

Uploading a Configuration

You can upload a configuration file to the access point from your hard drive or a mapped network drive, or you can upload a configuration from a file server.

Uploading from a Local Drive

Follow these steps to upload a configuration file from your hard drive or a mapped network drive:

Step 1 Follow the link path in the browser interface to reach the System Configuration Setup page.

Step 2 If you know the exact path and filename of the configuration file, type it in the Additional System Configuration File entry field.

If you aren't sure of the exact path to the configuration file, click **Browse...** next to the entry field. When the File Upload window appears, go to the directory that contains the configuration file and select the file. Click **Open**.

Step 3 When the filename appears in the Additional System Configuration File entry field, click **Browser Update Now**.

The configuration file is loaded and applied in the access point.

Uploading from a File Server

Follow these steps to upload a configuration file from a file server:

Step 1 Before you load a configuration file from a server, you need to enter FTP settings for the server. If you have already entered the FTP settings, skip to Step 3.

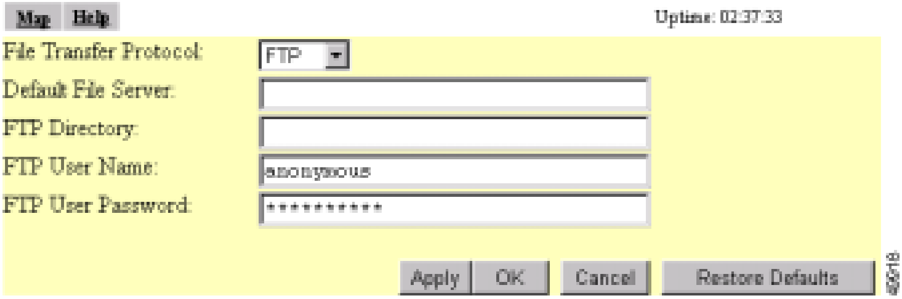
Follow this link path in the browser interface to reach the FTP Setup page:

a. On the Summary Status page, click **Setup**

b. On the Setup page, click **FTP**

The FTP Setup page appears. Figure 6-10 shows the FTP Setup page.

Figure 6-10 FTP Setup Page



Uptime: 02:37:33

File Transfer Protocol: FTP

Default File Server:

FTP Directory:

FTP User Name: anonymous

FTP User Password: **********

Step 2 Enter the FTP settings on the FTP Setup page.

a. Select FTP or TFTP from the File Transfer Protocol pull-down menu. FTP (File Transfer Protocol) is the standard protocol that supports transfers of data between local and remote computers. TFTP (Trivial File Transfer Protocol) is a relatively slow, low-security protocol that requires no user name or password.

b. In the Default File Server entry field, enter the IP address of the server where the access point should look for FTP files.

c. In the FTP Directory entry field, enter the directory on the server where FTP files are located.

d. In the FTP User Name entry field, enter the user name assigned to the FTP server. If you selected TFTP, you can leave this field blank.

e. In the FTP Password entry field, enter the password associated with the user name. If you selected TFTP, you can leave this field blank.

f. Click **OK**. You return automatically to the Setup page.

Step 3 Follow the link path in the web browser to reach the System Configuration Setup page.

Step 4 Click **Read Config File From Server**. The management system checks the server for several possible configuration filenames while attempting to load the configuration file. If the management system doesn't find the first filename, it continues to the next until it finds the file and loads it. It checks the server for the following names in the following order:

a. [system name].ini

b. [IP address].ini

c. [boot file from DHCP/BOOTP server].ini

d. [boot file from DHCP/BOOTP server].ini by TFTP

Resetting the Configuration

You can reset the access point configuration to the default settings without resetting the access point's IP identity, or you can reset the configuration to the default settings including the IP identity. If you reset the access point's IP identity, however, you might lose your browser connection to the access point.

Two buttons on the System Configuration Setup page reset the configuration to defaults:

- Reset System Factory Defaults Except IP Identity—this button returns all access point settings to their factory defaults *except*:
  - The access point's IP address, subnet mask, default gateway, and boot protocol
  - The users in the User Manager list
  - The SNMP Administrator Community name
- Reset All System Factory Defaults—this button returns all access point settings to their factory defaults *except*:
  - The users in the User Manager list
  - The SNMP Administrator Community name

Note To completely reset all access point settings to defaults, follow the steps in the "Resetting to the Default Configuration" section on page 9-44.

Follow these steps to reset the configuration to default settings:

Step 1 Follow the link path to reach the System Configuration Setup page. Figure 6-9 shows the System Configuration Setup page. The link path is listed under Figure 5-9.

Step 2 Click **Reset System Factory Defaults Except IP Identity** to reset the access point configuration to the default settings without resetting the access point's IP identity. Click **Reset All System Factory Defaults** to reset the configuration to the default settings including the IP identity.

Note If you reset the access point's IP identity, you might lose your browser connection to the access point.

Restarting the Access Point

Use the System Configuration Setup page to restart the access point.

- Click **"Warm" Restart System Now** to perform a warm restart of the access point. A warm restart reboots the access point.
- Click **"Cold" Restart System Now** to perform a cold restart of the access point. A cold restart is the equivalent of removing and then reapplying power for the access point.

Management System Setup

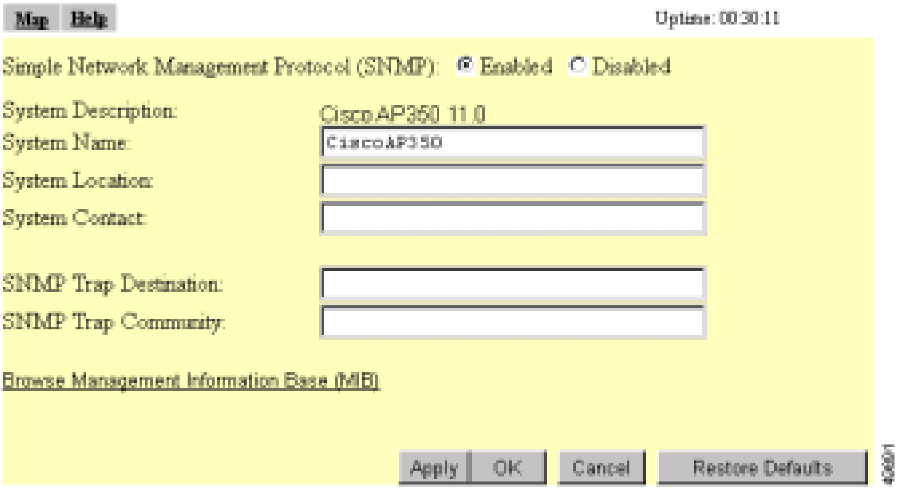
This chapter explains how to set up your access point to use SNMP, Telnet, or the console port to manage the access point. This chapter contains the following sections:

- SNMP Setup, page 7-2
- Console and Telnet Setup, page 7-5

SNMP Setup

Use the SNMP Setup page to configure the access point to work with your network's SNMP station. Figure 7-1 shows the SNMP Setup page.

Figure 7-1 SNMP Setup Page



Uptime: 00:30:11

Simple Network Management Protocol (SNMP): ● Enabled ○ Disabled

System Description: Cisco AP350 11.0

System Name: CiscoAP350

System Location:

System Contact:

SNMP Trap Destination:

SNMP Trap Community:

Browse Management Information Base (MIB)

Follow this link path to reach the SNMP Setup page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **SNMP** in the Services section of the page.

Settings on the SNMP Setup Page

The SNMP Setup page contains the following settings:

- Simple Network Management Protocol (SNMP)—Select **Enabled** to use SNMP with the access point.
- System Description—The system's device type and current version of firmware.

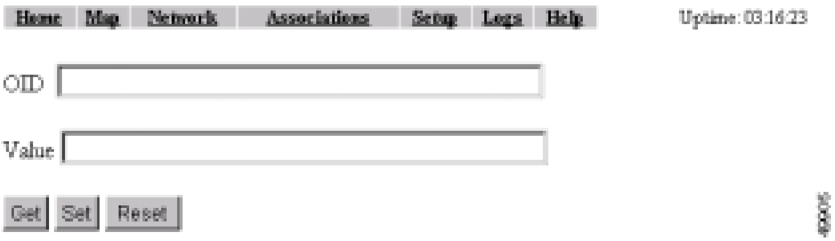
- System Name—The name of the access point. The name in this field is reported to your SNMP's management station as the name of the device when you use SNMP to communicate with the access point.
- System Location—Use this field to describe the physical location of the access point, such as the building or room in which it is installed.
- System Contact—Use this field to name the system administrator responsible for the access point.
- SNMP Trap Destination—The IP address of the SNMP management station. If your network uses DNS, enter a host name that resolves into an IP address.
- SNMP Trap Community—The SNMP community name required by the trap destination before it records traps sent by the access point.

The Browse Management Information Base (MIB) link at the bottom of the SNMP Setup page leads to the Database Query page.

Using the Database Query Page

Use the Database Query page to to find and change the value of many access point managed objects. Figure 7-2 shows the Database Query page.

Figure 7-2 Database Query Page



Follow this link path to reach the Database Query page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **SNMP** in the Services section of the page.
3. On the SNMP Setup page, click **Browse Management Information Base (MIB)**.

Settings on the Database Query Page

The Database Query page contains the following entry fields and buttons:

- OID—Type the object identifier (OID) in the OID field. You can use the integer or ASCII version of the OID. If you use the integer version of the OID, you must type the entire OID string (1.3.7.2.13.78.5.6, for example). If you use the ASCII name, you can often use the object's name as specified in the appropriate MIB (enableSNMP, for example).
- Value—When you click **Get**, the object's value appears in the Value field. If you want to assign a value to an object, you type an SNMP value in this field and click **Set**.
- Get—Click **Get** to find an object's value.
- Set—Click **Set** to assign a value to an object.
- Reset—Click **Reset** to return the page to default settings.

Changing Settings with the Database Query Page

Follow these steps to change an access point setting from the Database Query page:

Step 1 Type the object identifier (OID) in the OID field. You can use the integer or ASCII version of the OID. If you use the integer version of the OID, you must type the entire OID string (*1.3.7.2.13.78.5.6*, for example). If you use the ASCII name, you can often use the object's name as specified in the appropriate MIB (*enableSNMP*, for example). MIBs supported by the access point are listed in the "Supported MIBs" section on page 2-11.

Step 2 Click **Get**. The current value for the setting appears in the Value field.

Step 3 Modify the value in the Value field.

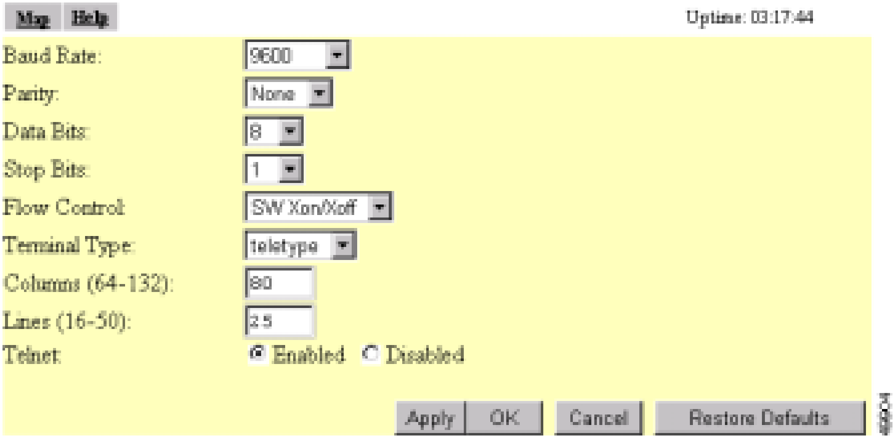
Step 4 Click **Set**. The new value is set on the access point.

Note If the object is read-only, the value is not changed when you click **Set**.

Console and Telnet Setup

Use the Console/Telnet Setup page to configure the access point to work with a terminal emulator or through Telnet. Figure 7-3 shows the Console/Telnet Setup page.

Figure 7-3 Console/Telnet Setup Page



Uptime: 03:17:44

Baud Rate:	9600
Parity:	None
Data Bits:	8
Stop Bits:	1
Flow Control:	SW Xon/Xoff
Terminal Type:	teletype
Columns (64-132):	80
Lines (16-50):	25
Telnet:	● Enabled ○ Disabled

Follow this link path to reach the Console/Telnet Setup page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Console/Telnet** in the Services section of the page.

Settings on the Console/Telnet Page

The Console/Telnet Setup page contains the following settings:

- Baud Rate—The rate of data transmission expressed in bits per second. Select a baud rate from 110 to 115,200, depending on the capability of the computer you use to open the access point management system.
- Parity—An error-detecting process based on the addition of a parity bit to make the total number of bits Odd or Even. The default setting, None, uses no parity bit.

- Data Bits—The default setting is 8.
- Stop Bits—The default setting is 1.
- Flow Control—Defines the way that information is sent between pieces of equipment to prevent loss of data when too much information arrives at the same time on one device. The default setting is SW Xon/Xoff.
- Terminal Type—The preferred setting is ANSI, which offers graphic features such as reverse video buttons and underlined links. Not all terminal emulators support ANSI, so the default setting is Teletype.
- Columns—Defines the width of the terminal emulator display within the range of 64 characters to 132 characters. Adjust the value to get the optimum display for your terminal emulator.
- Lines—Defines the height of the terminal emulator display within the range of 16 characters to 50 characters. Adjust the value to get the optimum display for your terminal emulator.
- Enable Telnet—The default setting is Yes. Select **No** to prevent Telnet access to the management system.

CHAPTER 8

Special Configurations

This chapter describes how to set up the access point in network roles other than as a root unit on a wired LAN. You can set up an access point as a repeater to extend the range of a wireless network, and you can use Hot Standby mode to use an access point as a backup unit in areas where you need extra reliability. Both configurations require two access points that support and rely upon each other.

This chapter contains the following sections:

- Setting Up a Repeater Access Point, page 8-1
- Using Hot Standby Mode, page 8-6

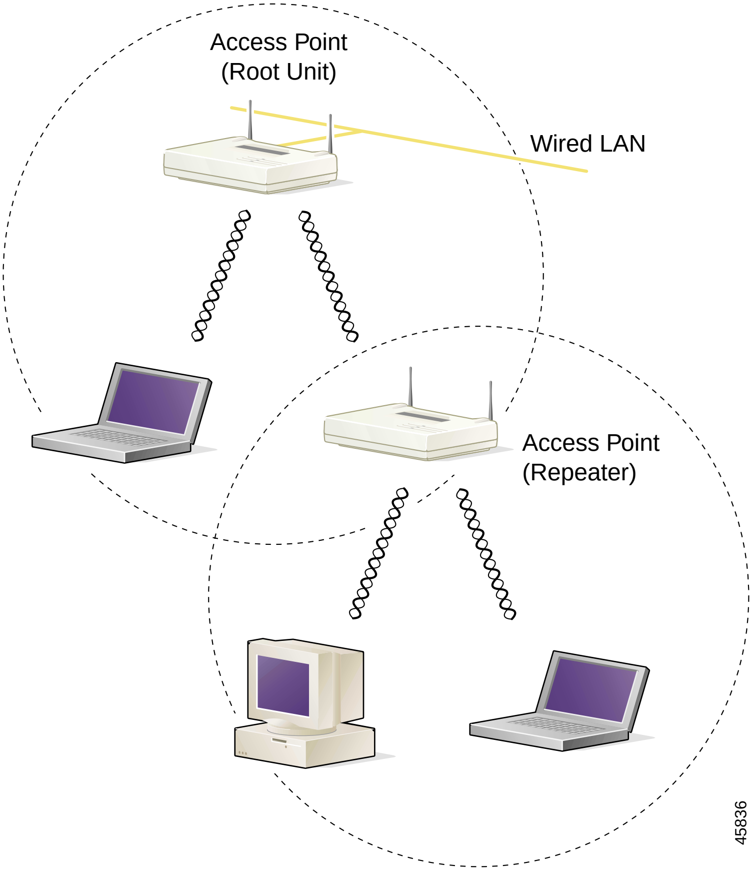
Setting Up a Repeater Access Point

A repeater access point is not connected to the wired LAN; it is placed within radio range of an access point connected to the wired LAN to extend the range of your infrastructure or to overcome an obstacle that blocks radio communication.

The repeater forwards traffic between wireless users and the wired LAN by sending packets to either another repeater or to an access point connected to the wired LAN. The data is sent through the route that provides the greatest performance for the client. When you configure an access point as a repeater, the access point's Ethernet port does not forward traffic. Figure 8-1 shows an access point acting as a repeater.

Note Non-Cisco client devices might have difficulty communicating with repeater access points.

Figure 8-1 Access Point as Repeater



You can set up a chain of several repeater access points, but throughput for client devices at the end of the repeater chain will be quite low. Because each repeater must receive and then re-transmit each packet on the same channel, throughput is cut in half for each repeater you add to the chain.

Omni-directional antennas, like the ones that ship with your access point, are best suited for repeater access points.

If you use EAP authentication on your wireless network, you can set up the repeater access point to authenticate using LEAP. See the "Setting up a Repeater Access Point as a LEAP Client" section on page 4-27 for instructions on enabling LEAP on a repeater.

Follow these steps to set up a repeater access point:

Step 1 Use the *Quick Start Guide: Cisco Aironet Access Points* and the information in this manual to set up an access point as a root unit on the wired LAN.

Step 2 Write down the root-unit access point's MAC address. The MAC address appears on the label on the bottom of the access point.

Step 3 The repeater access point will need to duplicate some of the root access point's settings. If the root access point has been completely configured, browse to the root access point and write down the following settings so you can refer to them when you set up the repeater access point:

- SSID (found on the Express Setup page)
- Default IP Subnet Mask (also on the Express Setup page)

Note You can also rely on the DHCP server to assign a default IP subnet mask.

- Default Gateway (also on the Express Setup page)

Note You can also rely on the DHCP server to assign a default gateway.

- Data rates (found on the AP Radio Hardware page)
- WEP settings (found on the AP Radio Data Encryption page)
- Authentication Types (found on the AP Radio Data Encryption page)

If the root access point settings have not been changed from the factory defaults, you don't need to write them down. If you reconfigure the root access point, however, you must enter the same settings on the repeater access point.

Step 4 Place the repeater access point within radio range of the root access point.

Step 5 For a 340 series access point, plug one end of the power cord into the access point's power connector. Plug the other end into an electrical outlet.

Step 6 For a 350 series access point, plug an Ethernet cable into the access point's Ethernet port. Plug the other end of the Ethernet cable into the side of the power injector labelled *To AP*.

Note The repeater access point will not be connected to the wired LAN, so do not run Ethernet cable from the power injector to a switch.

Step 7 Plug the power injector's power cable into an electrical outlet.

Note Step 8, Step 9, and Step 10 describe opening the access point management system using a terminal emulator, but you can use a crossover cable instead. Use a crossover cable to connect the access point's Ethernet port to the Ethernet connection on a computer and browse to the access point's IP address. If you use a crossover cable to open the management system, skip to Step 11.

Step 8 Attach a nine-pin, male-to-female, straight-through serial cable to the access point's serial port. Plug the other end of the serial cable into the COM 1 or COM 2 port on a computer.

Step 9 Use a terminal emulator to open the access point's management system. Assign these port settings to the terminal emulator: 9600 baud, 8 data bits, No parity, 1 stop bit, and Xon/Xoff flow control.

Step 10 When the terminal emulator connects with the access point, press = to display the access point's Summary Status page. If the repeater access point has never been configured before, the Express Setup page will appear instead of the Summary Status page.

Step 11 On the Express Setup page, enter the same SSID that is set on the root access point.

Note Step 12 and Step 13 describe assigning a static IP address, subnet mask, and gateway to the repeater. However, you can rely on your DHCP server to assign these settings if you do not need them to remain fixed. If the repeater will use the DHCP server, skip to Step 14.

Step 12 On the Express Setup page, enter a fixed IP address for the repeater access point in the Default IP address field.

Step 13 Also on the Express Setup page, enter the same settings in the Default IP Subnet Mask and Default Gateway fields that are on the root access point.

Step 14 On the Boot Server Setup page, select **none** for the Configuration Server Protocol. This setting will maintain a fixed IP address for the repeater access point.

If the root access point configuration has not been changed from the factory defaults, skip to Step 18.

Step 15 On the AP Radio Hardware page, enter the same settings for Data Rates that are on the root access point.

Step 16 On the AP Radio Data Encryption page, enter the same WEP key settings that are on the root access point.

Step 17 Also on the AP Radio Data Encryption page, select the same Authentication Types that are on the root access point.

Step 18 On the AP Radio Advanced page, enter the root access point's MAC address in the Specified access point 1 entry field.

Step 19 On the Express Setup page, select **Repeater Access Point** as the Role in Radio Network. The access point reboots when you apply this setting.

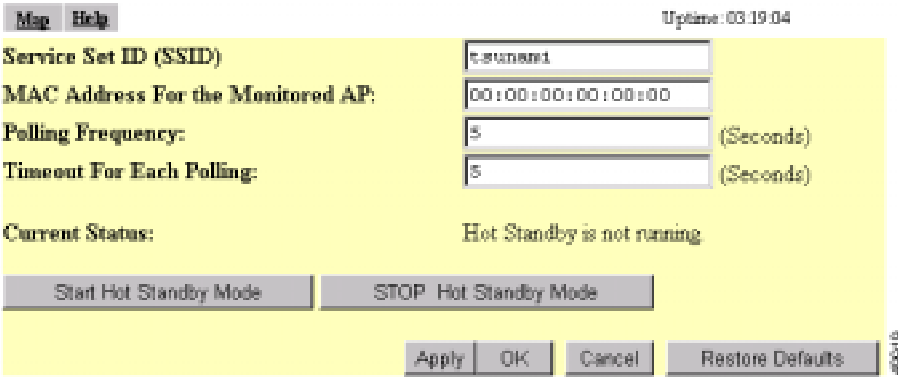
Step 20 The status LED on the root access point should be steady green, indicating that at least one client device is associated with it. The status LED on the repeater access point is steady green when it is associated with the root access point and has client devices associated with it. The repeater's status LED is steady for 7/8 of a second and off for 1/8 of a second when it is associated with the root access point but has no client devices associated with it. The repeater access point should also appear as associated with the root access point in the root access point's Association Table.

Using Hot Standby Mode

Hot Standby mode designates an access point as a backup for another access point. The standby access point is placed near the access point it monitors, configured exactly the same as the monitored access point. The standby access point associates with the monitored access point as a client and queries the monitored access point regularly through both the Ethernet and the radio. If the monitored access point fails to respond, the standby access point comes online and takes the monitored access point's place in the network.

Except for the IP address, the standby access point's settings should be identical to the settings on the monitored access point. You use the Hot Standby page to set up the standby access point. Figure 8-2 shows the Hot Standby page.

Figure 8-2 Hot Standby Page



Uptime: 03:19:04

Service Set ID (SSID) tsunami

MAC Address For the Monitored AP: 00:00:00:00:00:00

Polling Frequency: 5 (Seconds)

Timeout For Each Polling: 5 (Seconds)

Current Status: Hot Standby is not running

Follow this link path to reach the Hot Standby page:

- On the Summary Status page, click **Setup**.
- On the Setup page, click **Cisco Services** under Services.
- On the Cisco Services Setup page, click **Hot Standby Management**.

Note Wireless client devices associated to the standby access point lose their connections during the hot standby setup process.

Follow these steps to enable Hot Standby mode:

Step 1 On the standby access point, duplicate the settings that are entered on the monitored access point. Critical settings include:

- SSID (found on the Express Setup page)
- Default IP Subnet Mask (also on the Express Setup page)
- Default Gateway (also on the Express Setup page)
- Data rates (found on the AP Radio Hardware page)
- WEP settings (found on the AP Radio Data Encryption page)
- Authentication Types (found on the AP Radio Data Encryption page)

Step 2 On the standby access point, browse to the AP Radio Identification page:

a. On the Summary Status page, click **Setup**.

b. On the Setup page, click **Identification** in the AP Radio row under Network Ports.

Step 3 Select **no** for the Adopt Primary Port Identity option and click **Apply**. The access point reboots.

Step 4 After the access point reboots, browse to the Hot Standby page.

Step 5 Enter the monitored access point’s SSID in the Service Set ID entry field.

Step 6 Enter the monitored access point’s MAC address in the MAC Address For the Monitored AP entry field.

Step 7 Enter the number of seconds between each query the standby access point sends to the monitored access point.

Step 8 Enter the number of seconds the standby access point should wait for a response from the monitored access point before it assumes that the monitored access point has malfunctioned.

Step 9 Click **Start Hot Standby Mode**. The standby access point becomes a client device associated to the monitored access point.

Step 10 Click the browser’s refresh button to verify that the Current State line on the Hot Standby Setup page states that Hot Standby is initialized.

Note If the monitored access point malfunctions and the standby access point takes its place, repeat the hot standby setup on the standby access point when you repair or replace the monitored access point. The standby access point does not revert to standby mode automatically.

CHAPTER 9

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

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

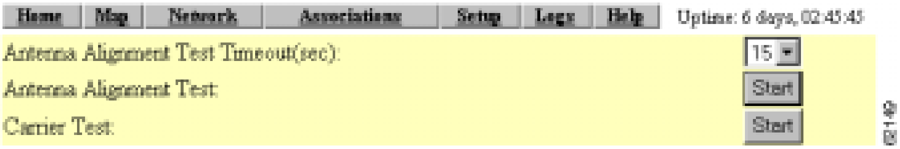
- The Radio Diagnostics Page provides the antenna alignment test and carrier test utilities.
- The Network Ports Page lists statistics on data transmitted and received by the access point.
- The Event Log Page lists network events.

Each page is described in the sections below.

Radio Diagnostics Page

Use the Radio Diagnostics page to test antenna alignment between two wireless networking devices and to examine the radio spectrum in which the access point operates. The antenna alignment test helps you find the best alignment for a repeater access point's directional antenna, and 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. Figure 9-1 shows the Radio Diagnostics page.

Figure 9-1 Radio Diagnostics Page



Antenna Alignment Test Timeout(sec): 15

Antenna Alignment Test:

Carrier Test:

Follow this link path to reach the Radio Diagnostics page:

1. On the Summary Status page, click **Diagnostics** in the Network Ports row.
2. On the Cisco Network Diagnostics page, click **Radio Diagnostics Tests**.

Antenna Alignment Test

The antenna alignment test measures signal strength and quality between a repeater access point and other wireless networking devices. For best results during the antenna alignment test, turn off all wireless networking devices within range of the access point except the device with which you are trying to align the access point’s antenna. Watch the constantly updated display in the Alignment Test window as you adjust the antenna.

You can run the antenna alignment test only on access points configured with the following Role in Radio Network settings:

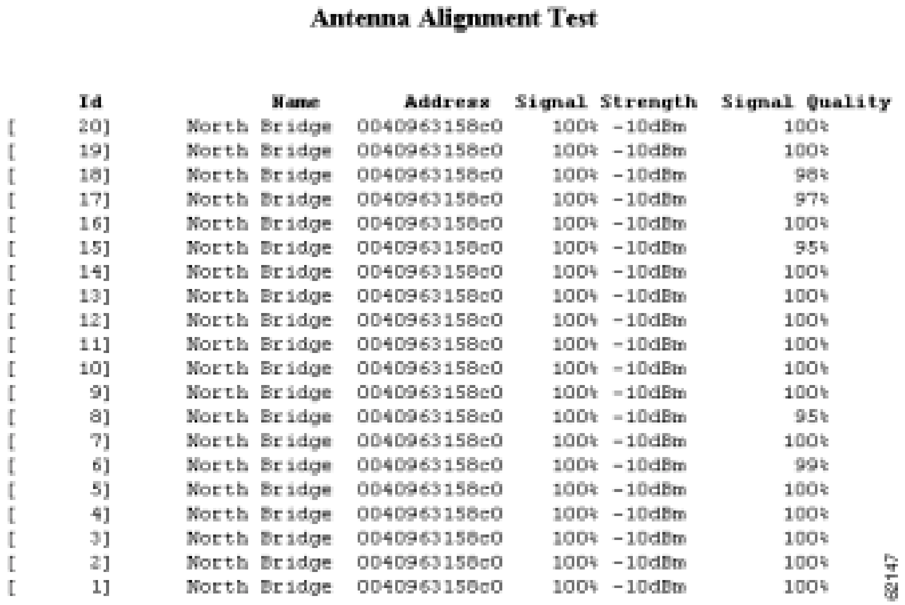
- Repeater Access Point
- Site Survey Client

To run the antenna alignment test on a root access point, change the Role in Radio Network setting on the Express Setup page.

Choose the number of seconds you want the alignment test to run from the Antenna Alignment Test Timeout pull-down menu. Choose a test duration of 15, 30, 45, or 60 seconds.

The Antenna Alignment Test window appears when you click **Start Antenna Alignment Test**, and the access point begins to send broadcast probe packets. Wireless networking devices with the same SSID as the access point send probe responses to the access point, and the access point measures the quality of the signal between the devices. Figure 9-2 shows an example Antenna Alignment Test window.

Figure 9-2 Antenna Alignment Test Window



Antenna Alignment Test

```
      Id              Name        Address   Signal Strength  Signal Quality
[     20]      North Bridge  0040963158c0     100% -10dBm         100%
[     19]      North Bridge  0040963158c0     100% -10dBm         100%
[     18]      North Bridge  0040963158c0     100% -10dBm          98%
[     17]      North Bridge  0040963158c0     100% -10dBm          97%
[     16]      North Bridge  0040963158c0     100% -10dBm         100%
[     15]      North Bridge  0040963158c0     100% -10dBm          95%
[     14]      North Bridge  0040963158c0     100% -10dBm         100%
[     13]      North Bridge  0040963158c0     100% -10dBm         100%
[     12]      North Bridge  0040963158c0     100% -10dBm         100%
[     11]      North Bridge  0040963158c0     100% -10dBm         100%
[     10]      North Bridge  0040963158c0     100% -10dBm         100%
[      9]      North Bridge  0040963158c0     100% -10dBm         100%
[      8]      North Bridge  0040963158c0     100% -10dBm          95%
[      7]      North Bridge  0040963158c0     100% -10dBm         100%
[      6]      North Bridge  0040963158c0     100% -10dBm          99%
[      5]      North Bridge  0040963158c0     100% -10dBm         100%
[      4]      North Bridge  0040963158c0     100% -10dBm         100%
[      3]      North Bridge  0040963158c0     100% -10dBm         100%
[      2]      North Bridge  0040963158c0     100% -10dBm         100%
[      1]      North Bridge  0040963158c0     100% -10dBm         100%
```

In this example, only one wireless networking device is in range of the access point, making it easy to see the relevant data. If results for several devices were displayed, it would be difficult to focus on the device with which you were trying to align the access point’s antenna.

Each data sample is listed in the data columns. The columns provide the following information:

- ID—The sequence number of the data sample. The most recent sample appears at the top of the column.
- Name—The system name of each device in the alignment test.
- Address—The MAC address of each device in the alignment test.
- Signal Strength—The signal strength between the access point and the other device. The left side of the Strength column displays the percentage of signal strength between the access point and the other device, and the right side of the column displays signal strength in dBm.

- Signal Quality—The quality of the signal link between the access point and the other device.

Carrier Test

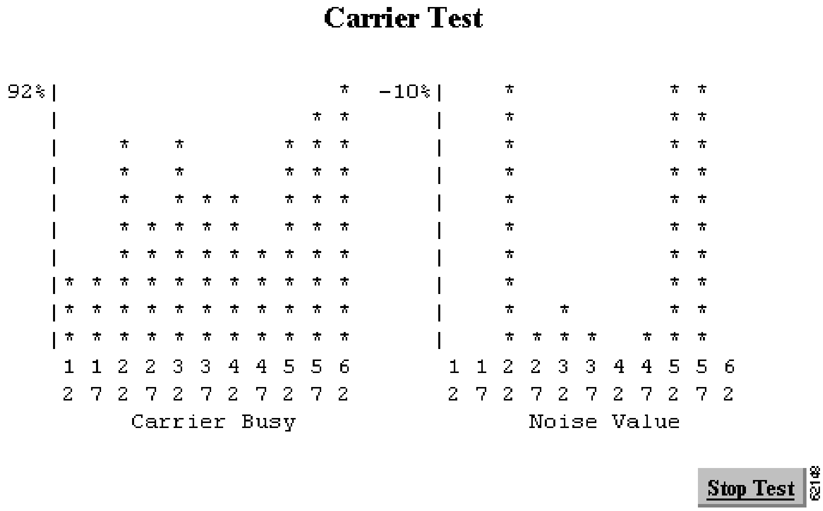
The carrier test measures the amount of radio activity on each frequency available to the access point. Use the carrier test to determine the best frequency for the access point to use. When you conduct a carrier test, make sure all wireless networking devices within range of the access point are operating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

When you click **Start Carrier Test**, 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 9-3 shows an example Carrier Test window.

Figure 9-3 Carrier Test Window



Carrier Test

```
92%|                     *   -10%|     *           * *
   |                   * *       |     *           * *
   |     *   *       * * *       |     *           * *
   |     *   *       * * *       |     *           * *
   |     *   * * *   * * *       |     *           * *
   |     * * * * *   * * *       |     *           * *
   |     * * * * * * * * *       |     *           * *
   | * * * * * * * * * * *       |     *           * *
   | * * * * * * * * * * *       |     *   *       * *
   | * * * * * * * * * * *       |     * * * *   * * *
     1 1 2 2 3 3 4 4 5 5 6         1 1 2 2 3 3 4 4 5 5 6
     2 7 2 7 2 7 2 7 2 7 2         2 7 2 7 2 7 2 7 2 7 2
          Carrier Busy                  Noise Value
```

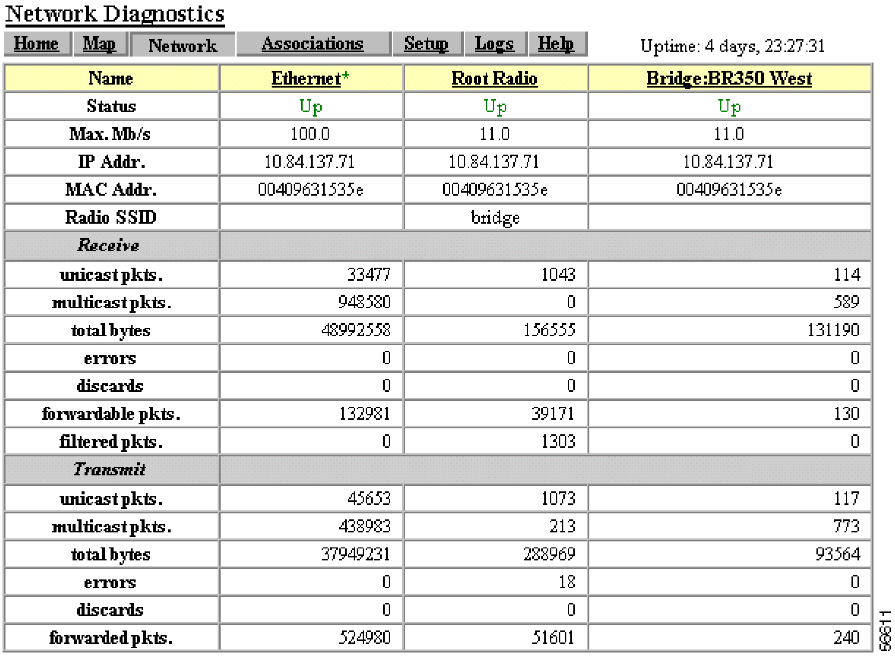
The bar graph on the left side of the window displays the percentage used for each frequency; the highest current percentage used is labeled on the top left of the graph. In this example, the highest percentage used for any frequency is 92. The access point's available frequencies are listed vertically 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.

Network Ports Page

The Network Ports page contains a table listing information for the access point's Ethernet and radio ports. Figure 9-4 shows a Network Ports page example.

Figure 9-4 Network Ports Page



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 Network Diagnostics link at the top of the Network Ports page leads to the Cisco Network Diagnostics page, where you can select diagnostic tests.

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 9-10 for information on the Ethernet Port page and the "AP Radio Page" section on page 9-13 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 3-19 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.

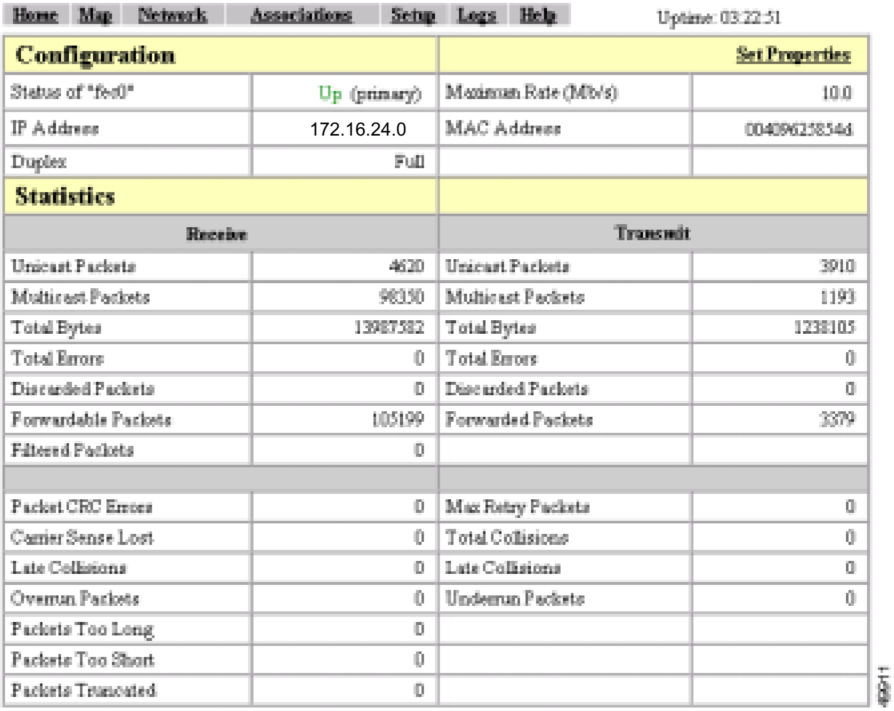
Data Transmitted

- 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 9-5 shows an Ethernet Port page example.

Figure 9-5 Ethernet Port Page



Uptime: 03:22:51

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		

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.

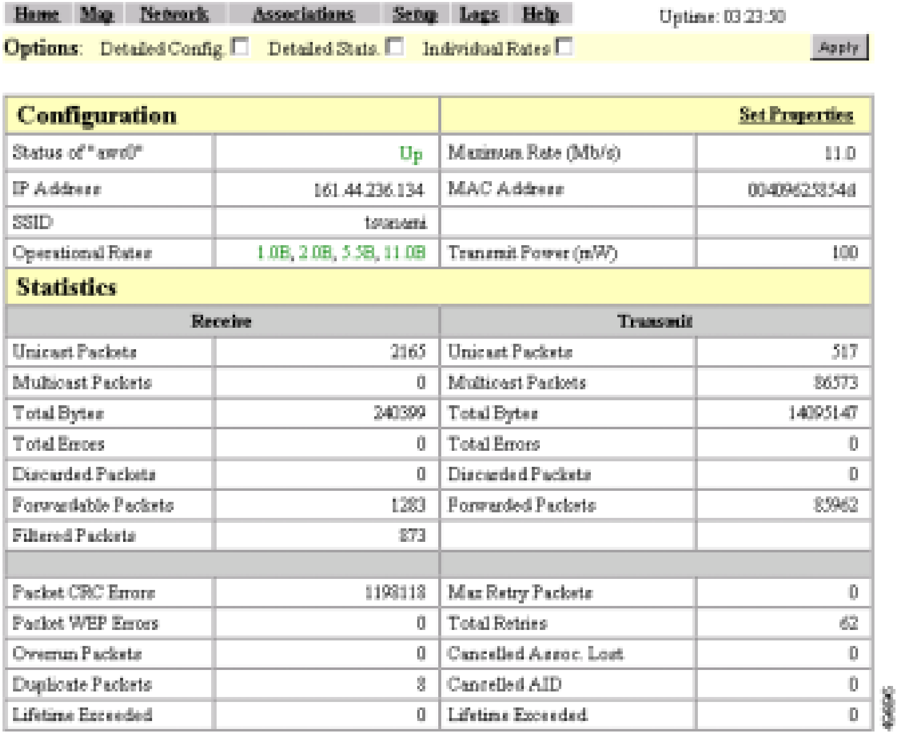
Transmit Statistics

- 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 9-6 shows an AP Radio Port page example.

Figure 9-6 AP Radio Port Page



Configuration			
Status of "awc0"	Up	Maximum Rate (Mb/s)	11.0
IP Address	161.44.236.134	MAC Address	00409623854d
SSID	tsunami		
Operational Rates	1.0B, 2.0B, 5.5B, 11.0B	Transmit Power (mW)	100
Statistics			
Receive		**Transmit**	
Unicast Packets	2165	Unicast Packets	517
Multicast Packets	0	Multicast Packets	86573
Total Bytes	240399	Total Bytes	14095147
Total Errors	0	Total Errors	0
Discarded Packets	0	Discarded Packets	0
Forwardable Packets	1283	Forwarded Packets	85962
Filtered Packets	873		
Packet CRC Errors	1198118	Max Retry Packets	0
Packet WEP Errors	0	Total Retries	62
Overrun Packets	0	Cancelled Assoc. Lost	0
Duplicate Packets	8	Cancelled AID	0
Lifetime Exceeded	0	Lifetime Exceeded	0

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 3-21 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.

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.

Display Options

Figure 9-6 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**.

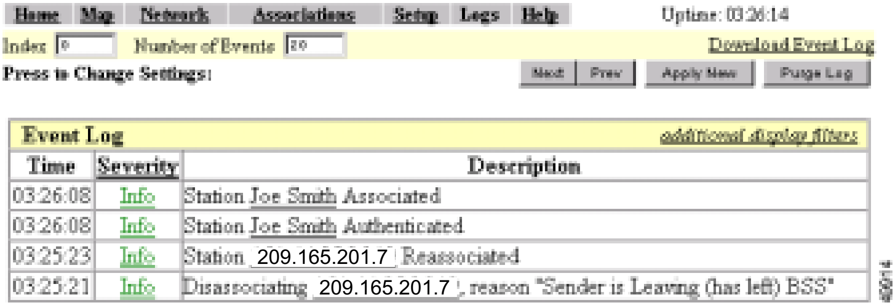
The display options include:

- 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 9-7 shows an Event Log page example.

Figure 9-7 Event Log Page



Uptime: 03:26:14

Index 0 Number of Events 20

Event Log

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"

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.

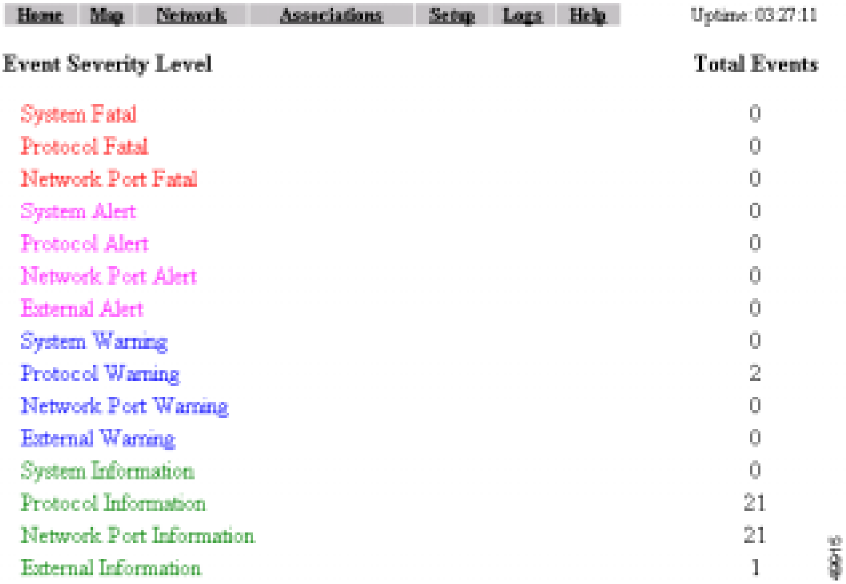
Saving the Log

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 9-8 shows an Event Log Summary page example.

Figure 9-8 Event Log Summary Page



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

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 9-1 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 9-1 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_arpshow	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
:vxdiag_ipstatshow	IP statistics
:vxdiag_memshow	free and allocated memory on the access point
:vxdiag_muxshow	networking protocols installed on the access point
:vxdiag_routeshow	current routing information
:vxdiag_tcpstatshow	TCP statistics
:vxdiag_udpstatshow	UDP statistics

Note The :eap_diag1_on and :eap_diag1_on EAP diagnostic commands are available in firmware versions 11.08 and later. The :vxdiag_arpshow, hostshow, ipstatshow, muxshow, routeshow, tcpstatshow, and udpstatshow commands are available in firmware version 11.11T. You can download the latest access point firmware version on Cisco.com at http://www.cisco.com/public/sw-center/sw-wireless.shtml.

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 2-6 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 9-1.

: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 9-21 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 9-21 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 9-2 for a list of flags

Table 9-2 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 9-21 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 9-21 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 9-21 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
tSysIntegri1b188          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 9-21 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 9-21 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 9-21 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: rptr 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: rptr Unit: 2
```

Follow the steps in the "Entering Diagnostic Commands" section on page 9-21 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 9-2 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 9-21 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 9-21 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 9-21 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 3-8.

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 9-34 and the "Tracing Packets for Ethernet and Radio Ports" section on page 9-35 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 9-34 or the "Tracing Packets for Ethernet and Radio Ports" section on page 9-35 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 9-36. 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 9-35.

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 insantly 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 9-36 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 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 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 2-5 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 9-9 shows the indicators on an access point with a plastic case, and Figure 9-10 shows the indicators on an access point with a metal case. Table 9-3 lists the meanings of the indicator signals.

Figure 9-9 Indicator Lights on Access Point with Plastic Case

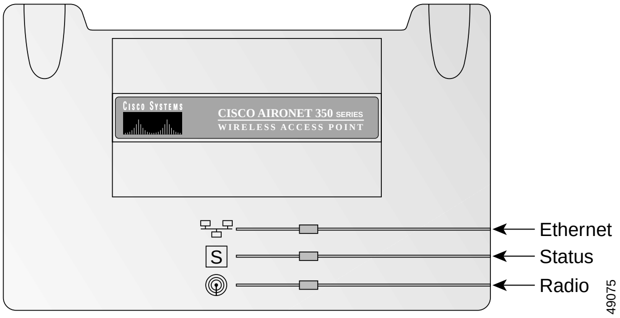
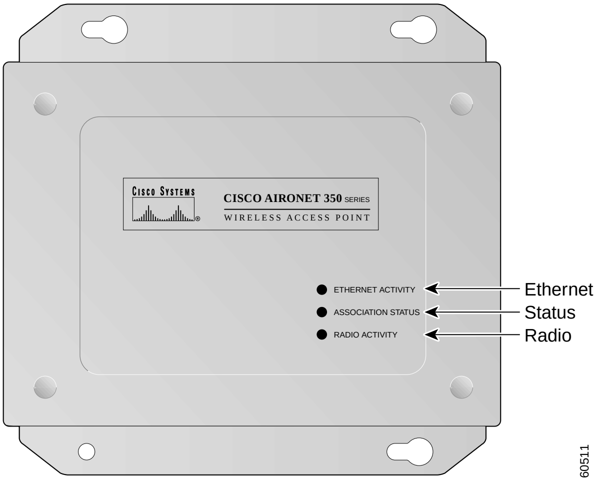


Figure 9-10 Indicator Lights on Access Point with Metal Case



- 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 9-3 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:

a. On the Summary Status page, click **Setup**.

b. 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 4-9 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 9-4 lists firmware versions for Cisco Aironet products and the draft with which they comply.

Table 9-4 802.1x 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	—

Table 9-4 802.1x Protocol Drafts and Compliant Client Firmware

Firmware Version	Draft 7	Draft 8	Draft 10
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.

a. On the Summary Status page, click **Setup**.

b. On the Setup page, click **Security**.

c. 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 6-15 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 HyperTeminal; 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 6-15 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 9-47. 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 9-49.

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 9-46.

⚠ **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 HyperTeminal; 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 9-46.

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 HyperTeminal; 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 accidently 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.

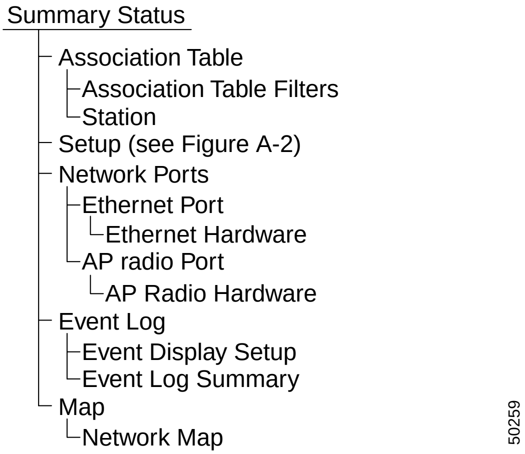
Step 16 When the Express Setup screen appears, begin reconfiguring the access point using the terminal emulator or an Internet browser.

APPENDIX A

Menu Tree

This section provides a menu tree for the Access Point management pages. The pages are organized the same way for all interfaces. Figures A-1 through A-4 show the organization for the management system's home page and the main sub-pages.

Figure A-1 Home Page Menu Tree



- Summary Status
  - Association Table
    - Association Table Filters
    - Station
  - Setup (see Figure A-2)
  - Network Ports
    - Ethernet Port
      - Ethernet Hardware
    - AP radio Port
      - AP Radio Hardware
  - Event Log
    - Event Display Setup
    - Event Log Summary
  - Map
    - Network Map

Figure A-2 Main Setup Page Menu Tree

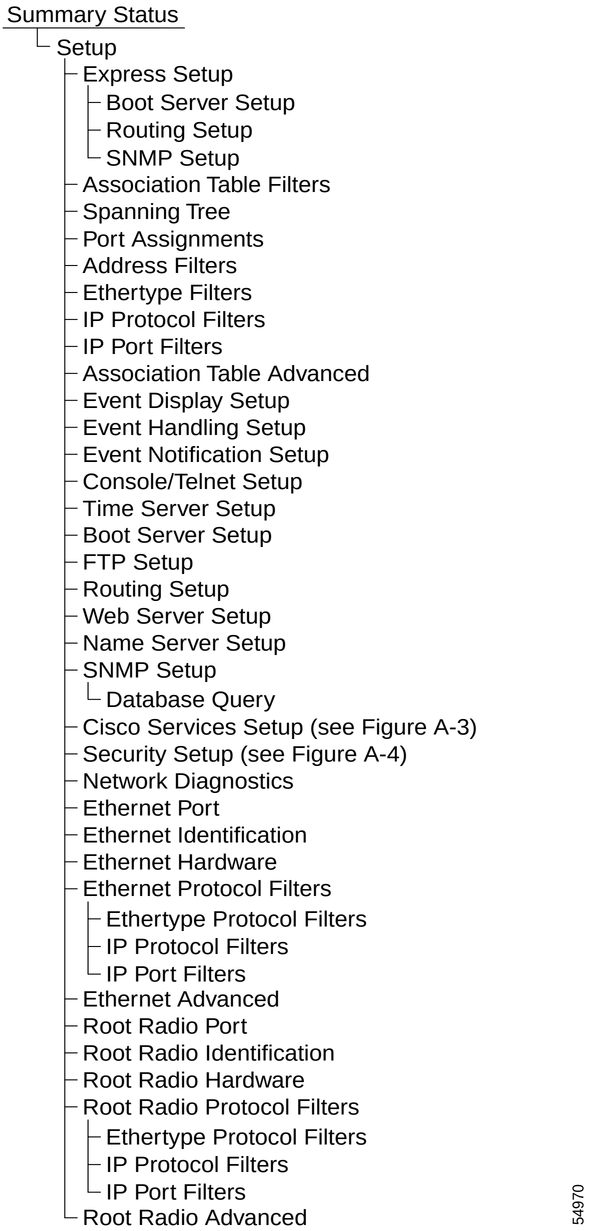


Figure A-3 Cisco Services Setup Page Menu Tree

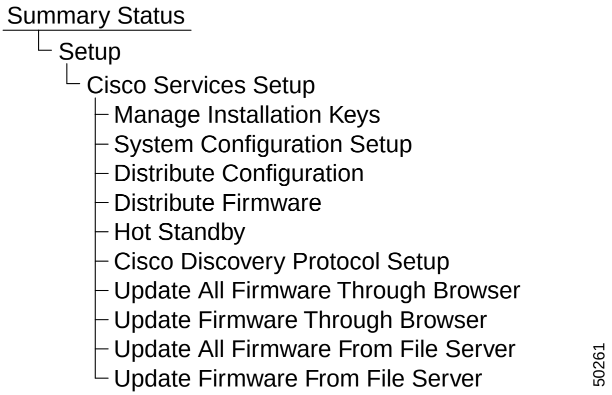
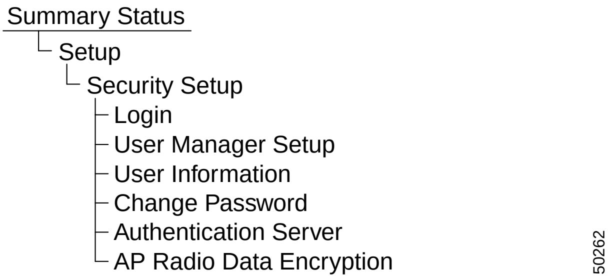

Summary Status
Setup
Cisco Services Setup
Manage Installation Keys
System Configuration Setup
Distribute Configuration
Distribute Firmware
Hot Standby
Cisco Discovery Protocol Setup
Update All Firmware Through Browser
Update Firmware Through Browser
Update All Firmware From File Server
Update Firmware From File Server
50261

Figure A-4 Security Setup Page Menu Tree



Protocol Filter Lists

The tables in this appendix list the protocols available on the Protocol Filters pages described in the "Protocol Filtering" section on page 3-8. The tables include:

- Table B-1, Protocols on the Ethertype Filters Page
- Table B-2, Protocols on the IP Protocol Filters Page
- Table B-3, Protocols on the IP Port Protocol Filters Page

In each table, the Protocol column lists the protocol name, and the Additional Identifier column lists other names for the same protocol. You can type either name in the Special Cases field on the Filter Set page to select the protocol. Table B-3 also lists the protocols' ISO numeric designators. You can use these designators to select a protocol also.

Table B-1 Protocols on the Ethertype Filters Page

Protocol	Additional Identifier	ISO Designator
ARP	—	0x0806
RARP	—	0x8035
IP	—	0x0800
Berkeley Trailer Negotiation	—	0x1000
LAN Test	—	0x0708
X.25 Level3	X.25	0x0805
Banyan	—	0x0BAD
CDP	—	0x2000
DEC XNS	XNS	0x6000
DEC MOP Dump/Load	—	0x6001
DEC MOP	MOP	0x6002
DEC LAT	LAT	0x6004
Ethertalk	—	0x809B
Appletalk ARP	Appletalk AARP	0x80F3
IPX 802.2	—	0x00E0
IPX 802.3	—	0x00FF
Novell IPX (old)	—	0x8137
Novell IPX (new)	IPX	0x8138
EAPOL (old)	—	0x8180
EAPOL (new)	—	0x888E
Telxon TXP	TXP	0x8729
Aironet DDP	DDP	0x872D
Enet Config Test	—	0x9000
NetBUI	—	0xF0F0

Table B-2 Protocols on the IP Protocol Filters Page

Protocol	Additional Identifier	ISO Designator
dummy	—	0
Internet Control Message Protocol	ICMP	1
Internet Group Management Protocol	IGMP	2
Transmission Control Protocol	TCP	6
Exterior Gateway Protocol	EGP	8
PUP	—	12
CHAOS	—	16
User Datagram Protocol	UDP	17
XNS-IDP	IDP	22
ISO-TP4	TP4	29
ISO-CNLP	CNLP	80
Banyan VINES	VINES	83
Encapsulation Header	encap_hdr	98
Spectralink Voice Protocol	SVP Spectralink	119
raw	—	255

Table B-3 Protocols on the IP Port Protocol Filters Page

Protocol	Additional Identifier	ISO Designator
TCP port service multiplexer	tcpmux	1
echo	—	7
discard (9)	—	9
systat (11)	—	11
daytime (13)	—	13
netstat (15)	—	15
Quote of the Day	qotd quote	17
Message Send Protocol	msp	18
ttytst source	chargen	19
FTP Data	ftp-data	20
FTP Control (21)	ftp	21
Secure Shell (22)	ssh	22
Telnet	—	23
Simple Mail Transport Protocol	SMTP mail	25
time	timserver	37
Resource Location Protocol	RLP	39
IEN 116 Name Server	name	42
whois	nicname 43	43
Domain Name Server	DNS domain	53
MTP	—	57
BOOTP Server	—	67
BOOTP Client	—	68
TFTP	—	69

Table B-3 Protocols on the IP Port Protocol Filters Page (continued)

Protocol	Additional Identifier	ISO Designator
gopher	—	70
rje	netrjs	77
finger	—	79
Hypertext Transport Protocol	HTTP www	80
ttylink	link	87
Kerberos v5	Kerberos krb5	88
supdup	—	95
hostname	hostnames	101
TSAP	iso-tsap	102
CSO Name Server	cso-ns csnet-ns	105
Remote Telnet	rtelnet	107
Postoffice v2	POP2 POP v2	109
Postoffice v3	POP3 POP v3	110
Sun RPC	sunrpc	111
tap ident authentication	auth	113
sftp	—	115
uucp-path	—	117
Network News Transfer Protocol	Network News readnews nntp	119
USENET News Transfer Protocol	Network News readnews nntp	119
Network Time Protocol	ntp	123

Table B-3 Protocols on the IP Port Protocol Filters Page (continued)

Protocol	Additional Identifier	ISO Designator
NETBIOS Name Service	netbios-ns	137
NETBIOS Datagram Service	netbios-dgm	138
NETBIOS Session Service	netbios-ssn	139
Interim Mail Access Protocol v2	Interim Mail Access Protocol IMAP2	143
Simple Network Management Protocol	SNMP	161
SNMP Traps	snmp-trap	162
ISO CMIP Management Over IP	CMIP Management Over IP cmip-man CMOT	163
ISO CMIP Agent Over IP	cmip-agent	164
X Display Manager Control Protocol	xdmcp	177
NeXTStep Window Server	NeXTStep	178
Border Gateway Protocol	BGP	179
Prospero	—	191
Internet Relay Chap	IRC	194
SNMP Unix Multiplexer	smux	199
AppleTalk Routing	at-rtmp	201
AppleTalk name binding	at-nbp	202
AppleTalk echo	at-echo	204
AppleTalk Zone Information	at-zis	206
NISO Z39.50 database	z3950	210
IPX	—	213

Table B-3 Protocols on the IP Port Protocol Filters Page (continued)

Protocol	Additional Identifier	ISO Designator
Interactive Mail Access Protocol v3	imap3	220
Unix Listserv	ulistserv	372
syslog	—	514
Unix spooler	spooler	515
talk	—	517
ntalk	—	518
route	RIP	520
timeserver	timed	525
newdate	tempo	526
courier	RPC	530
conference	chat	531
netnews	—	532
netwall	wall	533
UUCP Daemon	UUCP uucpd	540
Kerberos rlogin	klogin	543
Kerberos rsh	kshell	544
rfs_server	remotefs	556
Kerberos kadmin	kerberos-adm	749
network dictionary	webster	765
SUP server	supfilesrv	871
swat for SAMBA	swat	901
SUP debugging	supfiledbg	1127
ingreslock	—	1524
Prospero non-priveleged	prospero-np	1525
RADIUS	—	1812

Table B-3 Protocols on the IP Port Protocol Filters Page (continued)

Protocol	Additional Identifier	ISO Designator
Concurrent Versions System	CVS	2401
Cisco IAPP	—	2887
Radio Free Ethernet	RFE	5002

APPENDIX C

Channels, Power Levels, and Antenna Gains

This appendix lists the channels supported by the world's regulatory domains as well as the maximum power levels and antenna gains allowed per domain.

This appendix covers these topics:

Channels

The channel identifiers, channel center frequencies, and regulatory domains of each 22-MHz-wide channel are shown in Table C-1.

Table C-1 Channels

		Regulatory Domains				
Channel Identifier	Center Frequency	North America and ANZ	ETSI	Israel	China	Japan
1	2412 MHz	X	X	-	X	X
2	2417 MHz	X	X	-	X	X
3	2422 MHz	X	X	X	X	X
4	2427 MHz	X	X	X	X	X
5	2432 MHz	X	X	X	X	X
6	2437 MHz	X	X	X	X	X
7	2442 MHz	X	X	X	X	X
8	2447 MHz	X	X	X	X	X
9	2452 MHz	X	X	X	X	X
10	2457 MHz	X	X	-	X	X
11	2462 MHz	X	X	-	X	X
12	2467 MHz	-	X	-	-	X
13	2472 MHz	-	X	-	-	X
14	2484 MHz	-	-	-	-	X

Note Mexico is included in the North America regulatory domain; however, channels 1 through 8 are for indoor use only while channels 9 through 11 can be used indoors and outdoors. Users are responsible for ensuring that the channel set configuration is in compliance with the regulatory standards of Mexico.

Note France is included in the ETSI regulatory domain; however, channels 1 through 9 can be used in France at up to 10 mW EIRP, and channels 10 through 13 may be used at up to 100 mW EIRP. Users are responsible for ensuring that the channel set configuration is in compliance with the regulatory standards of France.

Maximum Power Levels and Antenna Gains

An improper combination of power level and antenna gain can result in equivalent isotropic radiated power (EIRP) above the amount allowed per regulatory domain. Table C-2 indicates the maximum power levels and antenna gains allowed for each regulatory domain.

Table C-2 Maximum Power Levels Per Antenna Gain

Regulatory Domain	Antenna Gain (dBi)	Maximum Power Level (mW)
North America and ANZ (4 watts EIRP maximum)	0	100
	2.2	100
	5.2	100
	6	100
	8.5	100
	12	100
	13.5	100
	21	20

Table C-2 Maximum Power Levels Per Antenna Gain (continued)

Regulatory Domain	Antenna Gain (dBi)	Maximum Power Level (mW)
ETSI (100 mW EIRP maximum)	0	100
	2.2	50
	5.2	30
	6	30
	8.5	5
	12	5
	13.5	5
	21	1
Israel (100 mW EIRP maximum)	0	100
	2.2	50
	5.2	30
	6	30
	8.5	5
	12	5
	13.5	5
	21	1
China (10 mW EIRP maximum)	0	5
	2.2	5
	5.2	n/a
	6	n/a
	8.5	n/a
	12	n/a
	13.5	n/a
	21	n/a

Table C-2 Maximum Power Levels Per Antenna Gain (continued)

Regulatory Domain	Antenna Gain (dBi)	Maximum Power Level (mW)
Japan (10 mW/MHz EIRP maximum)	0	50
	2.2	30
	5.2	30
	6	30
	8.5	n/a
	12	n/a
	13.5	5
	21	n/a

INDEX