CISCO SYSTEMS

Cisco Aironet
1200 Series Access Point
Software Configuration Guide

Software Release 11.50T
August, 2002

CONTENTS

Cisco Aironet 1200 Series Access Point Software Configuration Guide

Preface

The Cisco Aironet 1200 Series Access Point Software Configuration Guide describes how to configure Cisco Aironet 1200 Series Access Points using the web-based management system. This manual also briefly describes how to use the console-based management system.

Audience and Scope

This guide is for the network manager responsible for configuring a wireless network. Before using the material in this guide, you should be familiar with some of the concepts and terminology of Ethernet and wireless local area networking.

The scope of this guide is to provide the information you need to configure an access point, use the access point management system to browse to other devices on a wireless network, and troubleshoot problems with the access point that might arise.

Organization

This guide is organized into the following chapters:

Chapter 1, "Overview," is a functional overview of the access point management system. It describes the features of the management system and the access point's role in a wireless network.

Chapter 2, "Using the Management Interfaces," describes how to use the web-based and console-based management interfaces.

Chapter 3, "Configuration," describes the how to use the web-based management system to configure the access point.

Chapter 4, "Security Setup," describes how to set up and enable the access point's security features.

Chapter 5, "Network Management," describes how to use the web-based management system to browse to other devices on a wireless network.

Chapter 6, "Managing Firmware and Configurations," describes how to update the access point's firmware and use the management system to distribute firmware and configurations to other access points.

Chapter 7, "Management System Setup," describes methods of managing the access point other than through the access point management system.

Chapter 8, "Special Configurations," describes how to set up the access point in network roles other than as a root unit on a wired LAN, such as in repeater or Hot Standby mode.

Chapter 9, "Diagnostics and Troubleshooting," describes how to identify and resolve some of the problems that might arise when you configure an access point running this software release.

Appendix A, "Channels, Power Levels, and Antenna Gains," lists the channels supported by the world's regulatory domains.

Appendix B, "Protocol Filter Lists," lists the protocols you can select for filtering on the management system's Protocol Filters pages.

Conventions

This publication uses the following conventions to convey instructions and information:

Command descriptions use these conventions:

- Commands and keywords are in **boldface** text.

Notes, tips, and cautions use the following conventions and symbols:

Note Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in this manual.

🔍
Tip　　Means *the following are useful tips.*

⚠
Caution　Means *reader be careful.* In this situation, you might do something that could result in equipment damage or loss of data.

Related Publications

The following documents provide more information about access points and related products:

- *Quick Start Guide: Cisco Aironet 1200 Series Access Points* describes how to attach cables, power on, and assign an IP address and default gateway for the access point.

- *Cisco Aironet 1200 Series Access Point Hardware Installation Guide* describes the access point's hardware features, its physical and performance characteristics, and how to mount the access point on a wall, ceiling, or desktop. The *Cisco Aironet 1200 Series Access Point Hardware Installation Guide* also contains regulatory information for the device.

- *Cisco Secure Access Control Server for Windows 2000/NT Servers Version 2.6 User Guide* provides complete instructions for using Cisco Secure ACS, including steps for configuring Cisco Secure ACS to support access points.

- *Quick Start Guide: Cisco Aironet Wireless LAN Adapters* describes how to install and configure PC and PCI client adapter cards for use in a wireless LAN.

- *Cisco Aironet Wireless LAN Adapter Installation and Configuration Guide* provides hardware features, physical and performance characteristics, and installation instructions for PC and PCI Card client adapters. It also provides instructions for installing and using the wireless client adapter utilities.

Obtaining Documentation

These sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com

Translated documentation is available at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. In the Cisco Documentation home page, click the **Fax** or **Email** option in the "Leave Feedback" section at the bottom of the page.

You can e-mail your comments to bug-doc@cisco.com.

You can submit your comments by mail by using the response card behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages

- Order Cisco learning materials and merchandise

- Register for online skill assessment, training, and certification programs

If you want to obtain customized information and service, you can self-register on Cisco.com. To access Cisco.com, go to this URL:

http://www.cisco.com

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Cisco TAC inquiries are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.

- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.

- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.

- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

The Cisco TAC resource that you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

You can use the Cisco TAC Web Site to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

http://www.cisco.com/register/

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC Web Site, you can open a case online by using the TAC Case Open tool at this URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

■ **Obtaining Technical Assistance**

Overview

Cisco Aironet access points are wireless LAN transceivers that serve as the center point of a stand-alone wireless network or as the connection point between wireless and wired networks. In large installations, wireless users within radio range of an access point can roam throughout a facility while maintaining seamless, uninterrupted access to the network.

Your access point can contain two radios: a 2.4-GHz radio in an internal mini-PCI slot and a 5-GHz radio module in an external, modified cardbus slot. The access point supports one radio of each type, but it does not support two 2.4-GHz or two 5-GHz radios. You can configure the radios separately, using different settings on each radio.

The access point uses a browser-based management system, but you can also configure the access point using a terminal emulator, a Telnet session, or Simple Network Management Protocol (SNMP).

This chapter provides information on the following topics:

- Key Features, page 1-2
- Management Options, page 1-2
- Roaming Client Devices, page 1-3
- Network Configuration Examples, page 1-3

Key Features

This section describes the key features of the access point firmware. The following are the key features of this firmware version:

- Use accounting to collect data on wireless devices—You can enable accounting on the access point to send accounting data about wireless client devices to a RADIUS server on your network. See the "Enabling Wireless Network Accounting" section on page 5-16 for instructions on enabling accounting.

- Enable additional protection for WEP keys—You can enable three advanced security features to protect against sophisticated attacks on your wireless network's WEP keys: Message Integrity Check (MIC), WEP key hashing, and broadcast WEP key rotation. See the "Additional WEP Security Features" section on page 4-3 for more information on additional WEP protection.

- Use EAP to Authenticate Repeater Access Points—Set up repeater access points to authenticate to your network like other wireless client devices. After you provide a network username and password for the repeater, it authenticates to your network using LEAP, Cisco's wireless authentication method, and receives and uses dynamic WEP keys. See the "Setting up a Repeater Access Point as a LEAP Client" section on page 4-27 for instructions on setting up a repeater access point.

Management Options

You can use the access point management system through the following interfaces:

- A web-browser interface

- A command-line interface (CLI)

- Simple Network Management Protocol (SNMP)

The access point's management system pages are organized the same way for the web- browser interface and the CLI. The examples in this manual are all taken from the browser interface. Chapter 2, "Using the Management Interfaces" provides a detailed description of each management option.

Roaming Client Devices

If you have more than one access point in your wireless LAN, wireless client devices can roam seamlessly from one access point to another. The roaming functionality is based on signal quality, not proximity. When a client's signal quality drops, it roams to another access point.

Wireless LAN users are sometimes concerned when a client device stays associated to a distant access point instead of roaming to a closer access point. However, if a client's signal to a distant access point remains strong, the client will not roam to a closer access point. If client devices checked constantly for closer access points, the extra radio traffic would slow throughput on the wireless LAN.

Network Configuration Examples

This section describes the access point's role in three common wireless network configurations. The access point's default configuration is as a root unit connected to a wired LAN or as the central unit in an all-wireless network. The repeater role requires a specific configuration.

Root Unit on a Wired LAN

An access point connected directly to a wired LAN provides a connection point for wireless users. If more than one access point is connected to the LAN, users can roam from one area of a facility to another without losing their connection to the network. As users move out of range of one access point, they automatically connect to the network (associate) through another access point. The roaming process is seamless and transparent to the user. Figure 1-1 shows access points acting as root units on a wired LAN.

Figure 1-1   Access Points as Root Units on a Wired LAN
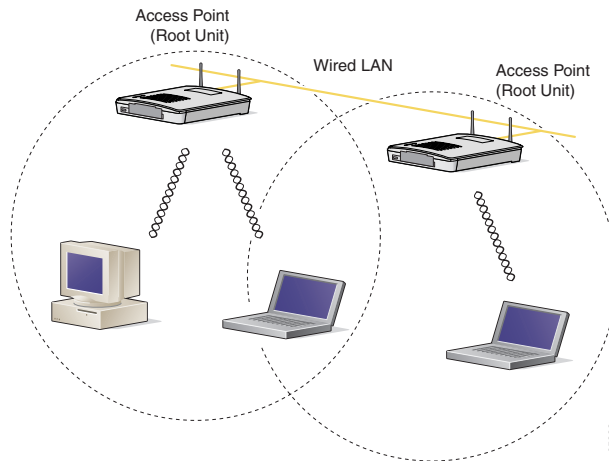
Repeater Unit that Extends Wireless Range

An access point can be configured as a stand-alone repeater 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 best performance for the client. You can set up either of the radios in your access point as a repeater, but one radio must be set up as a root unit.

Figure 1-2 shows an access point acting as a repeater. Consult the "Setting Up a Repeater Access Point" section on page 8-1 for instructions on setting up the access point as a repeater.

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

Figure 1-2   Access Point as Repeater
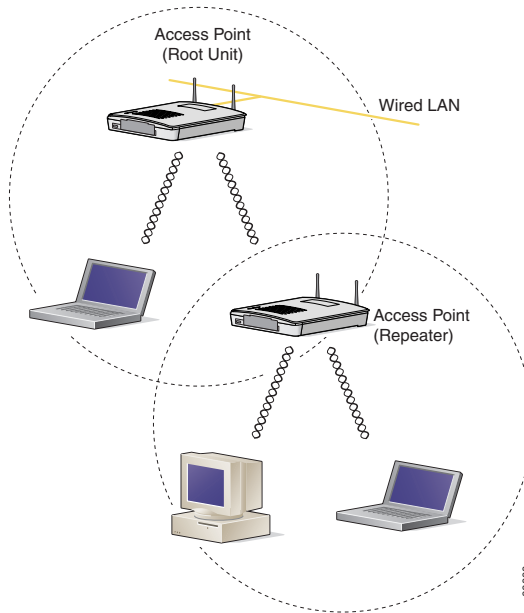
Central Unit in an All-Wireless Network

In an all-wireless network, an access point acts as a stand-alone root unit. The access point is not attached to a wired LAN; it functions as a hub linking all stations together. The access point serves as the focal point for communications, increasing the communication range of wireless users. Figure 1-3 shows an access point in an all-wireless network.

Figure 1-3   Access Point as Central Unit in All-Wireless Network
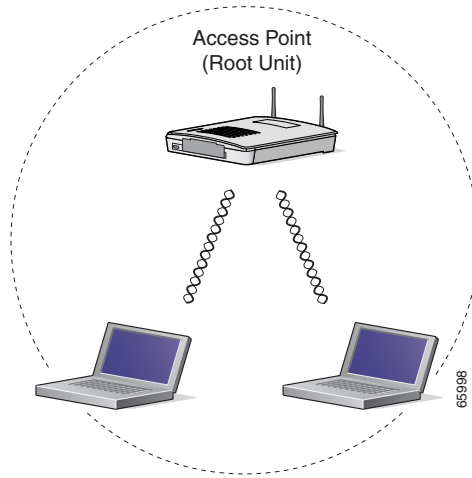
C H A P T E R **2**

Using the Management Interfaces

This chapter describes the interfaces you can use to configure the access point. You can use a web-browser interface, a command-line interface through a terminal emulator or a Telnet session, or a Simple Network Management Protocol (SNMP) application. The access point's management system web pages are organized the same way for the web browser and command-line interfaces. The examples in this manual show the web-browser interface.

This chapter contains the following sections:

Using the Web-Browser Interface

The web-browser interface contains management pages that you use to change access point settings, upgrade and distribute firmware, and monitor and configure other wireless devices on the network.

> **Note** The access point management system is fully compatible with Microsoft Internet Explorer versions 4.0 or later and Netscape Communicator versions 4.0 or later. Earlier versions of these browsers cannot use all features of the management system.

Using the Web-Browser Interface for the First Time

Use the access point's IP address to browse to the management system. See the *Quick Start Guide: Cisco Aironet 1200 Series Access Points* for instructions on assigning an IP address to the access point.

Follow these steps to begin using the web-browser interface:

Step 1 Start the browser.

Step 2 Enter the access point's IP address in the browser **Location** field (Netscape Communicator) or **Address** field (Internet Explorer) and press **Enter**.

If the access point has not been configured, the Express Setup page appears. If the access point has been configured, the Summary Status page appears.

Using the Management Pages in the Web-Browser Interface

The system management pages use consistent techniques to present and save configuration information. Navigation buttons appear at the top of the page, and configuration action buttons appear at the bottom. You use the navigation buttons to display other management pages, and you use the configuration action buttons to save or cancel changes to the configuration.

Note   It's important to remember that clicking your browser's Back button is the same as clicking **Cancel**: if you make changes on a management page, your changes are not applied when you click **Back**. Changes are only applied when you click **Apply** or **OK**.

Table 2-1 lists the page links and buttons that appear on most management pages.

Table 2-1   Common Buttons on Management Pages

Button/Link	Description
Navigation Links	
Home	Displays the Summary Status page.
Map	Opens the Map window, which contains links to every management page.
Network	Displays the Network Ports page.
Associations	Displays the Association Table page, which provides a list of all devices on the wireless network and links to the devices.
Setup	Displays the Setup page, which contains links to the management pages with configuration settings.
Logs	Displays the Event Log page, which lists system events and their severity levels.
Help	Displays the online help for the current window and the online help table of contents.
Login	Logs you into the access point's management system for access to all pages and features appropriate for your user level.
Configuration Action Buttons	
Apply	Saves changes made on the page and remain on the page.
OK	Saves changes made on the page and return to the previous page.
Cancel	Discards changes to the page and return to the previous page.
Restore Defaults	Returns all settings on the page to their default values.

Navigating Using the Map Windows

The Map window appears when you click **Map** at the top of any management page. You can use the Map window to jump quickly to any system management page, or to a map of your entire wireless network.

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

To display the sub-pages for each main page, click the bullet next to a main page link (Microsoft Internet Explorer), or click **expand** next to a main page link (Netscape Communicator). In Figure 2-1, the sub-pages for the Network Ports page are expanded.

Figure 2-1   Map Window with Network Ports Pages Expanded
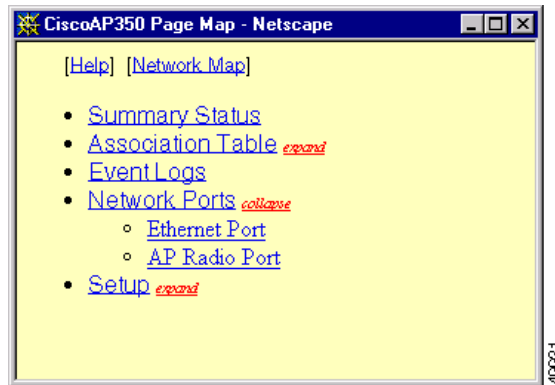
The Network Map window appears when you click **Network Map** in the Map window. You use the Network Map window to open a new browser window displaying information for any device on your wireless network. Figure 2-2 shows the Network Map window.

Figure 2-2   The Network Map Window
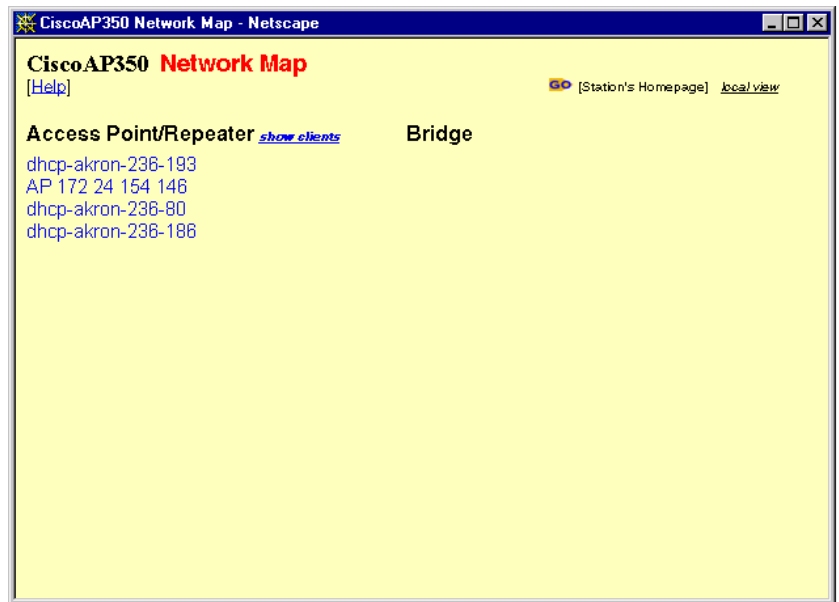
Click the name of a wireless device to open a new browser window displaying a Station page listing the access point's local information for that device. Click **Go** beside the device name to open a new browser window displaying that device's home page, if available. Some devices, such as PC Card clients, might not have home pages.

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 the Command-Line Interface

You can use a command-line interface (CLI) to configure your access point through a terminal emulation program or a Telnet session instead of through your browser. This section provides instructions for Microsoft's HyperTerminal and for Telnet; other programs are similar.

Preparing to Use a Terminal Emulator

To use a terminal emulator to open the CLI, you need to:

1. Connect a nine-pin, female DB-9 to RJ-45 serial cable to the RJ-45 serial port on the access point and to the COM port on a computer.

2. Set up a terminal emulator to communicate with the access point. Use the following settings for the terminal emulator connection: 9600 baud, 8 data bits, no parity, 1 stop bit, and no flow control.

   Use the Console/Telnet Setup page to adjust the console and Telnet connection settings. See the "Console and Telnet Setup" section on page 7-5 for details on the Console/Telnet Setup page.

Connecting the Serial Cable

Connect a DB-9 to RJ-45 serial cable to the COM port on a computer and to the RJ-45 serial port on the access point. Figure 2-3 shows the serial port connection.

Figure 2-3   Connecting the Serial Cable

DB-9 to RJ-45
serial cable

RJ-45 serial
connector
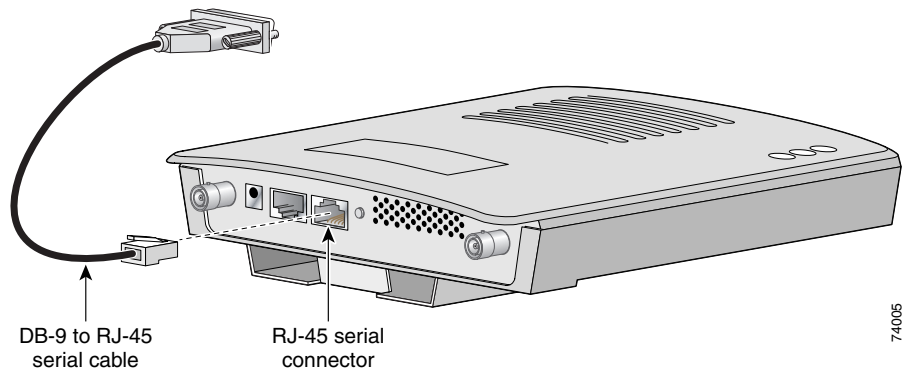
74005

Note The Cisco part number for the DB-9 to RJ-45 serial cable is AIR-CONCAB1200. Browse to http://www.cisco.com/go/marketplace to order a serial cable.

Setting Up the Terminal Emulator

Follow these steps to set up the terminal emulator:

Step 1   Open a terminal emulator.

Step 2   Enter these settings for the connection:

- Bits per second (baud rate): 9600
- Data bits: 8
- Parity: none
- Stop bits: 1
- Flow control: none

Step 3   Press **=** to display the home page of the access point. If the access point has not been configured before, the Express Setup page appears as the home page. If the access point is already configured, the Summary Status page appears as the home page.

Changing Settings with the CLI

The CLI pages use consistent techniques to present and save configuration information. Table 2-2 lists the functions that appear on most CLI pages.

Table 2-2   Common Functions on CLI Pages

Function	Description
Press **Enter** three times	Refreshes the page and cancel changes to settings.
Ctrl-R	Refreshes the page and cancel changes to settings.
=	Returns to the home page without applying changes.
:back	Moves back one page without applying changes.

Table 2-2   Common Functions on CLI Pages (continued)

Function	Description
:bottom	Jumps to the bottom of a long page, such as Event Log. When you are at the bottom of a page, this function becomes *:top*.
:down	Moves down one page length (24 lines) on a long page, such as Event Log. When you are at the bottom of a long page, this function becomes *:up*.

You can also enter diagnostic commands in the CLI. See the "Using Command-Line Diagnostics" section on page 9-20 for information on the CLI diagnostic commands.

Figure 2-4 shows a CLI page example.

Figure 2-4   CLI Page Example

```
CiscoAP350           Console/Telnet Setup      Uptime: 01:32:53

 [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 )][24   ]

 [Enable Telnet?][X]

 [Apply] [OK]   [Cancel] [Restore Defaults]
_____
[Home] - [Network] - [Associations] - [Setup] - [Logs] - [Help]
[END]




(Auto Apply On) :Back, ^R, =, <ENTER>, or [Link Text]:
```

Selecting Pages and Settings

When you type names and settings that appear in brackets you jump to that page or setting. HyperTerminal jumps to the page or setting as soon as it recognizes a unique name, so you only need to type the first few characters in the page or setting name. To jump from the home page to the Setup page, for example, you only need to type **se**.

Applying Changes to the Configuration

The CLI's auto-apply feature is on by default, so changes you make to any page are applied automatically when you move to another management page. To apply changes and stay on the current page, type **apply** and press **Enter**.

Using a Telnet Session

Follow these steps to browse to the CLI pages with Telnet:

Step 1   On your computer's Start menu, select **Programs > Accessories > Telnet**.

If Telnet is not listed in your Accessories menu, select **Start > Run**, type **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, type **open** followed by the access point's IP address.

Step 3   In the Host Name field, type the access point's IP address and click **Connect**.

Using SNMP

You use an SNMP management application to configure the access point with SNMP. Follow these steps to configure the access point with SNMP:

Step 1 Compile the MIB you need to use in your SNMP management application. MIBs supported by the access point are listed in Supported MIBs.

Step 2 Use a web browser, a Telnet session, or the console interface to open the Express Setup page in the access point management system.

Step 3 Enter an SNMP community name in the SNMP Admin. Community field and click **OK** or **Apply**.

Step 4 Follow this link path to reach the SNMP Setup page:

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

    b. On the Setup page, click **SNMP** in the Services section of the page.

Use the SNMP Setup page to enter detailed SNMP settings, such as the SNMP trap destination. See the "SNMP Setup" section on page 7-2 for details on the SNMP Setup page.

Supported MIBs

The access point supports the following MIBs:

- Standard MIB-II (RFC1213-MIB.my)

    Supported branches:

    - system (1.3.6.1.2.1.1)
    - interfaces (1.3.6.1.2.1.2)
    - ip (1.3.6.1.2.1.4)
    - tcp (1.3.6.1.2.1.6)
    - udp (1.3.6.1.2.1.7)
    - snmp (1.3.6.1.2.1.11)

To download this MIB, browse to
http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml and click
SNMP v1 MIBs. Scroll down the list of files and select **RFC1213-MIB.my**.

- Cisco Discovery Protocol MIB (CISCO-CDP-MIB-V1SMI.my)

    - Supported branch: ciscoCdpMIB (1.3.6.1.4.1.9.23)

    To download this MIB, browse to
    http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml and click
    SNMP v1 MIBs. Scroll down the list of files and select
    CISCO-CDP-MIB-V1SMI.my.

- Cisco Aironet Access Point MIB (AWCVX-MIB.my)

    - Supported branch: awcVx (1.3.6.1.4.1.522.3)

    You can download the latest release of the access point MIB at the following
    URL:

    http://www.cisco.com/public/sw-center/sw-wireless.shtml

- IEEE802dot11-MIB.my:

    - Supported branch: ieee802dot11 (1.2.840.10036)

    To download this MIB, browse to

    ftp://ftp.cisco.com/pub/mibs/v1/IEEE802dot11-MIB-V1SMI.my.

Using SNMP

Configuration

This chapter describes how to use the pages in the access point management system to configure the access point. The main Setup page provides links to all the pages containing access point settings.

This chapter contains the following sections:

Note See Chapter 4, "Security Setup" for information on setting up the access point's security features.

Basic Settings

This section describes the basic settings on the Express Setup page. If you need to set up an access point quickly with a simple configuration, or change or update a basic setting, you can enter all the access point's essential settings for basic operation on the Express Setup page.

The page contains radio settings for both the 2.4-GHz internal radio and the 5-GHz external radio module. You can configure the radios separately, using different settings on each radio. Figure 3-1 shows the Express Setup page.

Figure 3-1   Express Setup Page

Follow this link path to reach the Express Setup page:

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

2. On the Setup page, click **Express Setup**.

Entering Basic Settings

The Express Setup page contains the following settings:

- System Name
- MAC Address
- Configuration Server Protocol
- Default IP Address
- Default IP Subnet Mask
- Default Gateway
- Radio Service Set ID (SSID)
- Role in Radio Network
- Radio Network Optimization (Optimize Radio Network For)
- Radio Network Compatibility (Ensure Compatibility With)
- SNMP Admin. Community

System Name

The system name appears in the titles of the management system pages and in the access point's Association Table page. The system name is not an essential setting, but it helps identify the access point on your network.

MAC Address

The access point's Media Access Control (MAC) address appears under the system name. The MAC address is a unique serial number permanently assigned to the access point's Ethernet controller. You cannot change the access point's MAC address.

Configuration Server Protocol

Set the Configuration Server Protocol to match the network's method of IP address assignment. Click the Configuration Server link to jump to the Boot Server Setup page, which contains detailed settings for configuring the access point to work with your network's BOOTP or DHCP servers for automatic assignment of IP addresses.

The Configuration Server Protocol pull-down menu contains the following options:

- None—Your network does not have an automatic system for IP address assignment.
- BOOTP—With Bootstrap Protocol, IP addresses are hard-coded based on MAC addresses.
- DHCP—With Dynamic Host Configuration Protocol, IP addresses are "leased" for predetermined periods of time.

Default IP Address

Use this setting to assign or change the access point's IP address. If DHCP or BOOTP is not enabled for your network, the IP address you enter in this field is the access point's IP address. If DHCP or BOOTP is enabled, this field provides the IP address only if no server responds with an IP address for the access point.

Default IP Subnet Mask

Enter an IP subnet mask to identify the subnetwork so the IP address can be recognized on the LAN. If DHCP or BOOTP is not enabled, this field is the subnet mask. If DHCP or BOOTP is enabled, this field provides the subnet mask only if no server responds to the access point's DHCP or BOOTP request.

Default Gateway

Enter the IP address of your default internet gateway here. The entry 255.255.255.255 indicates no gateway. Clicking the Gateway link takes you to the Routing Setup page, which contains detailed settings for configuring the access point to communicate with the IP network routing system.

Radio Service Set ID (SSID)

The SSID is 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. Several access points on a network or sub-network can share an SSID. The SSID can be any alphanumeric, case-sensitive entry from two to 32 characters long.

This setting appears twice on the page, once for the internal radio and once for the external radio module. You can use the same setting or different settings for each radio.

Role in Radio Network

Use this pull-down menu to select the role of the access point on your network. This setting appears twice on the page, once for the internal radio and once for the external radio module. You can use the same setting or different settings for each radio.

The menu contains the following options:

- Root Access Point—A wireless LAN transceiver that connects an Ethernet network with wireless client stations. Use this setting if the access point is connected to the wired LAN. Figure 3-2 shows an access point operating as a root unit in a network.

Figure 3-2   Root-Unit Access Points
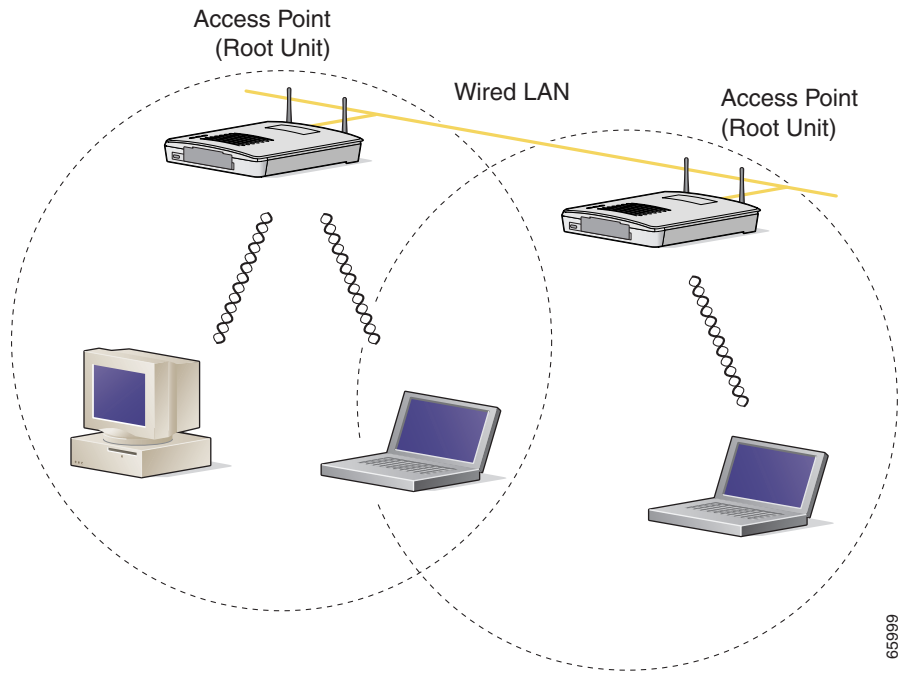
- Repeater Access Point—An access point that transfers data between a client and another access point or repeater. One or both access point radios can be set up as repeaters. Figure 3-3 shows an access point operating as a repeater in a network.

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

Figure 3-3   Repeater Access Point
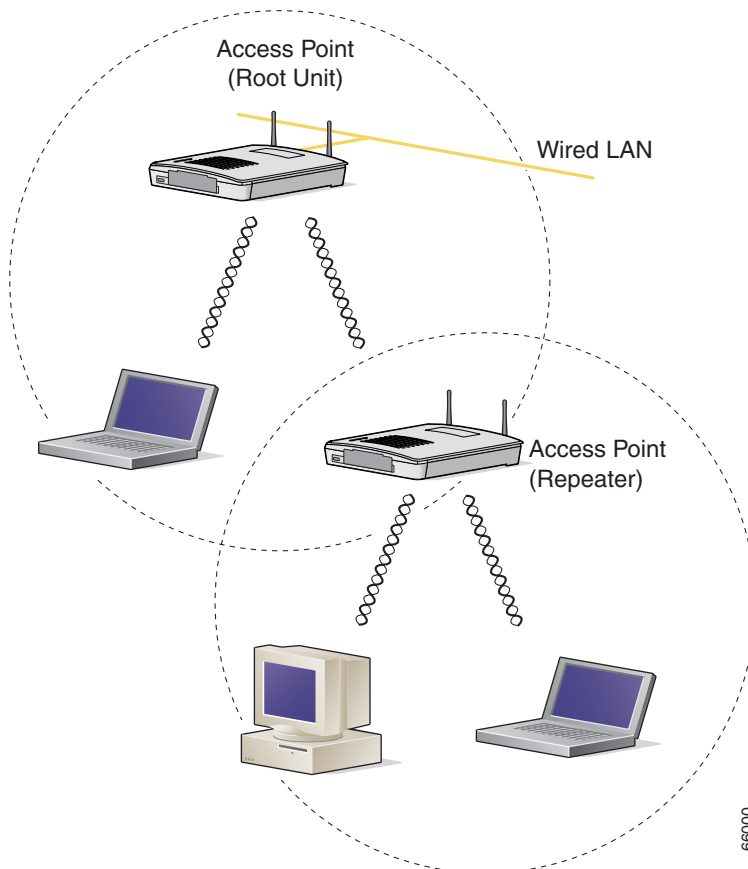
- Site Survey Client—A wireless device that depends on an access point for its connection to the network. Use this setting when performing a site survey for a repeater access point. When you select this setting, clients are not allowed to associate.

Radio Network Optimization (Optimize Radio Network For)

You use this setting to select either preconfigured settings for the access point radio or customized settings for the access point radio. This setting appears twice on the page, once for the internal radio and once for the external radio module. You can use the same setting or different settings for each radio.

- Default—Strikes a compromise between range and throughput, providing good range and good throughput.

- Throughput—Maximizes the data volume handled by the access point but might reduce the access point's range.

- Range—Maximizes the access point's range but might reduce throughput.

- Custom—The access point uses the settings you enter on the AP Radio Hardware page. Click **Custom** to go to the AP Radio Hardware page.

Radio Network Compatibility (Ensure Compatibility With)

You use this setting to automatically configure the access point to be compatible with other devices on your wireless LAN. This setting appears twice on the page, once for the internal radio and once for the external radio module. You can use the same setting or different settings for each radio.

- 2Mb/sec clients—Select this setting if your network contains Cisco Aironet devices that operate at a maximum speed of 2 Mbps.

- non-Aironet 802.11—Select this setting if there are non-Cisco Aironet devices on your wireless LAN.

SNMP Admin. Community

To use Simplified Network Management Protocol (SNMP), enter a community name here. This name automatically appears in the list of users authorized to view and make changes to the access point's management system, and SNMP is enabled.

Click the SNMP link to go to the SNMP Setup page, where you can edit other SNMP settings.

You can define other SNMP communities on the Administrator Authorization pages. See the "Setting Up Administrator Authorization" section on page 4-41 for instructions on using the Administrator Authorization pages.

Filter Setup

This section describes how to set up filtering to control the flow of data through the access point. You can filter data based on protocols and MAC addresses. Each type of filtering is explained in the following sections:

- Protocol Filtering, page 3-9
- MAC Address Filtering, page 3-14

Protocol Filtering

Protocol filters prevent or allow the use of specific protocols through the access point. You can set up individual protocol filters or sets of filters. You can filter protocols for wireless client devices, users on the wired LAN, or both. For example, an SNMP filter on the access point's radio port prevents wireless client devices from using SNMP with the access point but does not block SNMP access from the wired LAN.

Use the Ethernet Protocol Filters page to create and enable protocol filters for the access point's Ethernet port, and use the AP Radio Protocol Filters page to create and enable protocol filters for the access point's radio port. The pages are identical except for the page title. Figure 3-4 shows the main body for the pages.

Figure 3-4   Main Body for Protocol Filters Pages

Follow this link path to reach the Ethernet Protocol Filters page:

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

2. On the Setup page, click **Filters** in the Ethernet row under Network Ports.

Follow this link path to reach the AP Radio Protocol Filters page:

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

2. On the Setup page, click **Filters** in the AP Radio row under Network Ports.

The left side of the Protocol Filters page contains links to the Ethertype Filters, the IP Protocol Filters, and the IP Port Filters pages. These links also appear on the main Setup page under Associations. Use the Protocol Filters pages to assign protocols to a filter set. Table B-1, Table B-2, and Table B-3 in Appendix B list the protocols available on each page.

Creating a Protocol Filter

Follow these steps to create a protocol filter:

Step 1 Follow the link path to the Ethernet or AP Radio Protocol Filters page.

Step 2 Click **Ethertype**, **IP Protocol**, or **IP Port** to display the Filters page that contains the protocols you want to filter. Figure 3-5 shows the Filters page.

Figure 3-5   Filters Page

| Home | Map | Network | Associations | Setup | Logs | Help | Uptime: 01:07:18 |

Set ID: [   ]   Set Name: [   ]   [Add New]

Existing Ethertype Protocol Filter Sets:

[Edit]
[Remove]

Step 3   Enter a descriptive filter set name in the Set Name field.

Step 4   Enter an identification number in the Set ID entry field if you want to assign a specific SNMP identifier to the filter set. If you don't enter an ID, an SNMP identifier will be assigned to the set automatically, starting with 1 for the first filter set and incrementing by one for each additional set.

Step 5   Click **Add New**. The Filter Set page appears. Figure 3-6 shows the Filter Set page.

Figure 3-6   Filter Set Page

| Map | Help | Uptime: 01:11:36 |

Name: [test17]

Default Disposition: [forward ▼]

Default Time To Live (msec):
unicast: [0]   multicast: [0]

Special Cases: [   ]   [Add New]

Select an entry from below to [Edit] or [Remove]

| | | | Time-to-Live (msec) | | |
| select | Ethertype | Disposition | Priority | Unicast | Multicast | Alert? |

[Apply] [OK] [Cancel]   [Restore Defaults]

Step 6 Select **forward** or **block** from the Default Disposition pull-down menu. This setting is the default action for the protocols you include in the filter set. You can override this setting for specific protocols.

Step 7 In the Default Time to Live fields, enter the number of milliseconds unicast and multicast packets should stay in the access point's buffer before they are discarded. These settings will be the default time-to-live values for the protocols you include in the filter set, but you can override the settings for specific protocols. If you leave these settings at 0, the time-to-live settings default to 3 seconds for multicast packets and 5 seconds for unicast packets.

Step 8 Type the name or the ISO numeric designator for the protocol you want to add in the Special Cases entry field and click **Add New**. For example, to add Telnet to an IP port filter set, type **telnet** or **23**.

The Protocol Filter Set page appears. Figure 3-7 shows the Protocol Filter Set page.

Figure 3-7   Protocol Filter Set Page

Step 9 Select **forward** or **block** from the Disposition pull-down menu to forward or block the protocol traffic, or leave this setting at **default** to use the default disposition that you selected for the filter set in Step 6.

Step 10 Select a priority for the protocol from the Priority pull-down menu. The menu includes the following options:

- background—Use this setting for bulk transfers and other activities that are allowed on the network but should not impact network use by other users and applications.

- default—This setting is the same as best effort, which applies to normal LAN traffic.

- excellentEffort—Use this setting for a network's most important users.

- controlledLoad—Use this setting for important business applications that are subject to some form of admission control.

- interactiveVideo—Use this setting for traffic with less than 100 ms delay.

- interactiveVoice—Use this setting for traffic with less than 10 ms delay.

- networkControl—Use this setting for traffic that must get through to maintain and support the network infrastructure.

Step 11   Enter milliseconds in the Time-to-Live entry fields. If you leave these settings at 0, the protocol adopts the default time-to-live values you entered in Step 7.

> **Note**   The time-to-live values you enter should be compatible with the priority you select for the protocol. For example, if you select interactiveVoice as the priority and enter high time-to-live values, voice packets will stay in the access point buffer longer than necessary, causing delivery of stale, useless packets.

Step 12   Select *Alert?* **yes** to send an alert to the event log when a user transmits or receives the protocol through the access point.

Step 13   Click **OK**. The Filter Set page appears with the protocol listed at the bottom of the page.

To edit the protocol entry, type the protocol name in the Special Cases entry field or click the select button beside the entry and click **Edit**. To delete the protocol, type the protocol name in the Special Cases entry field or click the select button beside the entry and click **Remove**.

Step 14   To add another protocol to the filter set, repeat Step 8 through Step 13. When you have included all the protocols you need in the filter set, click **OK**. The EtherType Filters, IP Protocol Filters, or IP Port Filters page appears, and the filter sets you defined appear in the filter set list at the bottom of the page.

> ✎
>
> **Note**   After defining the protocol filter set, follow the steps in the Enabling a Protocol Filter section to activate the filter.

Enabling a Protocol Filter

Follow these steps to enable a protocol filter:

Step 1   Complete the steps listed in the "Creating a Protocol Filter" section on page 3-10 to define a protocol filter.

Step 2   Follow the link path to the Ethernet Protocol Filters page or the AP Radio Protocol Filters page.

Step 3   Select the protocol filter set that you want to enable from the Ethertype, IP Protocol, or IP Port pull-down menu.

Step 4   Click **OK**. The filter set is enabled.

MAC Address Filtering

MAC address filters allow or disallow the forwarding of unicast and multicast packets either sent from or addressed to specific MAC addresses. You can create a filter that passes traffic to all MAC addresses except those you specify, or you can create a filter that blocks traffic to all MAC addresses except those you specify.

> ✎
>
> **Note**   MAC address filters are powerful, and you can lock yourself out of the access point if you make a mistake setting up the filters. If you accidentally lock yourself out of your access point, follow the instructions in the "Using the Command-Line Interface" section on page 2-5 to use the CLI to disable the filters.

Use the Address Filters page to create MAC address filters for the access point. Figure 3-8 shows the Address Filters page.

Figure 3-8   Address Filters Page

Follow this link path to reach the Address Filters page:

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

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

Creating a MAC Address Filter

Follow these steps to create a MAC address filter:

Step 1   Follow the link path to the Address Filters page.

Step 2   Type a destination MAC address in the New MAC Address Filter: Dest MAC Address field. You can type the address with colons separating the character pairs (00:40:96:12:34:56, for example) or without any intervening characters (004096123456, for example).

✎

Note   If you plan to disallow traffic to all MAC addresses except those you specify as allowed, put your own MAC address in the list of allowed MAC addresses. If you plan to disallow multicast traffic, add the broadcast MAC address (ffffffffffff) to the list of allowed addresses.

Step 3   Click **Allowed** to pass traffic to the MAC address or click **Disallowed** to discard traffic to the MAC address.

Step 4   Click **Add**. The MAC address appears in the Existing MAC Address Filters list. To remove the MAC address from the list, select it and click **Remove**.

🔍

Tip   You can create a list of allowed MAC addresses on an authentication server on your network. Consult the "Setting Up MAC-Based Authentication" section on page 4-29 for instructions on using MAC-based authentication.

If you intend to list allowed MAC addresses on an authentication server, select **yes** for the *Look up MAC Address on Authentication Server if not in Existing Filter List* option.

Step 5   Click **OK**. You return automatically to the Setup page.

Step 6   To enable MAC address filtering on the internal radio, click **Advanced** in the AP Radio: Internal row of the Network Ports section at the bottom of the Setup page. To enable MAC address filtering on the external module radio, click **Advanced** in the AP Radio: Module row. The AP Radio Advanced page appears. Figure 3-9 shows the AP Radio Advanced page for the internal radio.

Figure 3-9   AP Radio Advanced Page for Internal Radio

Step 7   Select **Disallowed** from the pull-down menu for Default Unicast Address Filter. The access point discards all unicast traffic except packets sent to the MAC addresses listed as allowed on the Address Filters page.

Select **Allowed** from the pull-down menu for Default Unicast Address Filter if you want to allow traffic to all MAC addresses except those listed as disallowed on the Address Filters page.

Unicast packets are addressed to just one device on the network. *Multicast* packets are addressed to multiple devices on the network.

Select Disallowed or Allowed from the pull-down menu for Default Multicast Address Filter. The access point discards all multicast traffic except packets sent to the MAC addresses listed as allowed on the Address Filters page.

Step 8   Click **OK**. You return automatically to the Setup page.

If clients are not filtered immediately, click **WARM RESTART SYSTEM NOW** on the Manage System Configuration page to restart the access point. To reach the Manage System Configuration page, Click **Cisco Services** on the main Setup page and click **Manage System Configuration** on the Cisco Services Setup page.

> **Note**   The Ethernet Advanced page contains the Default Unicast and Multicast Address Filter settings for the Ethernet port. These settings work as described above, but you should use extra caution changing the settings on the Ethernet Advanced page because they can lock you out of your access point. To reach the Ethernet Advanced page, click **Advanced** in the Ethernet row of the Network Ports section at the bottom of the Setup page.

> **Note**   Client devices with blocked MAC addresses cannot send or receive data through the access point, but they might remain in the Association Table as unauthenticated client devices. Client devices with blocked MAC addresses disappear from the Association Table when the access point stops monitoring them or they associate with another access point. See the "Association Table Advanced Page" section on page 3-68 for information on setting a monitoring timeout for each device class.

Radio Configuration

This section describes how to configure the access point radios. You use the AP Radio pages in the management system to set the configuration for each radio. The radio pages include:

- AP Radio Identification pages—Contain the basic locating and identity information for the access point internal and module radio ports. See the "Entering Identity Information" section on page 3-19 for instructions on using the AP Radio Identification pages.

- AP Radio Hardware pages—Contain settings for the access point's SSID, data rates, transmit power, antennas, radio channel, and operating thresholds for the access point internal and module radio ports. See the "Entering Radio Hardware Information" section on page 3-22 for instructions on using the AP Radio Hardware pages.

- AP Radio Advanced pages—Contain settings for the operational status of the access point's internal and module radio ports. You can also use these pages to make temporary changes in port status to help with troubleshooting network problems. See the "Entering Advanced Configuration Information" section on page 3-31 for instructions on using the AP Radio Advanced pages.

- AP Radio Ports pages—List key information on the access point's radio ports.

Entering Identity Information

Use the AP Radio Identification pages to enter basic locating and identity information for the access point radios. The internal radio and the radio module both have an AP Radio Identity page. Both pages contain the same settings. Figure 3-10 shows the AP Radio Identification page for the internal radio.

Figure 3-10   The AP Radio Identification Page for the Internal Radio

Follow this link path to reach the AP Radio Identification page:

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

2. On the Setup page, click **Identification** in on eof the AP Radio rows under Network Ports.

Settings on the AP Radio Identification Page

The AP Radio Identification pages contain the following settings:

- Primary Port Settings
- Default IP Address
- Default IP Subnet Mask
- Service Set ID (SSID)
- LEAP User Name
- LEAP Password

The page also displays the access point's MAC address, the radio serial number, the radio's current IP address, the radio's current IP subnet mask, the maximum packet length that the radio can send and receive, the radio firmware version, and the radio boot block version.

Primary Port Settings

Two options allow you to designate the radio port as the Primary Port and select whether the radio port adopts or assumes the identity of the primary port.

- Primary Port?—The primary port determines the access point's MAC and IP addresses. Ordinarily, the access point's primary port is the Ethernet port, which is connected to the wired LAN, so this setting is usually set to no. Select **no** to set the Ethernet port as the primary port. Select **yes** to set the radio port as the primary port.

- Adopt Primary Port Identity?—Select **yes** to adopt the primary port settings (MAC and IP addresses) for the radio port. Select **no** to use different MAC and IP addresses for the radio port.

  Access points acting as root units adopt the primary port settings for the radio port. When you put an access point in standby mode, however, you select **no** for this setting. Some advanced wireless bridge configurations also require different identity settings for the radio port.

Default IP Address

Use this setting to assign an IP address for the radio port that is different from the access point's Ethernet IP address. During normal operation the radio port adopts the identity of the Ethernet port. When you put an access point in standby mode, however, you assign a different IP address to the radio port. Some advanced wireless bridge configurations also require a different IP address for the radio port.

Default IP Subnet Mask

Enter an IP subnet mask to identify the subnetwork so that the IP address can be recognized on the LAN. If DHCP or BOOTP is not enabled, this field is the subnet mask. If DHCP or BOOTP is enabled, this field provides the subnet mask only if no server responds to the access point's request.

The current IP subnet mask displayed under the setting shows the IP subnet mask currently assigned to the access point. This is the same subnet mask as the default subnet mask unless DHCP or BOOTP is enabled. If DHCP or BOOTP is enabled, this is the subnet mask used by the DHCP or BOOTP server.

You can also enter this setting on the Express Setup page.

Service Set ID (SSID)

The SSID is a 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. The SSID can be any alphanumeric entry from two to 32 characters long.

You can also enter this setting on the Express Setup page.

LEAP User Name

Use this field if the radio is set up as a repeater and authenticates to the network using LEAP. When the radio authenticates using LEAP, the access point sends this user name to the authentication server.

Follow the steps in the "Setting up a Repeater Access Point as a LEAP Client" section on page 4-27 to set up the radio as a LEAP client.

LEAP Password

Use this field if the radio is set up as a repeater and authenticates to the network using LEAP. When the radio authenticates using LEAP, the access point uses this password for authentication.

Follow the steps in the "Setting up a Repeater Access Point as a LEAP Client" section on page 4-27 to set up the radio as a LEAP client.

Entering Radio Hardware Information

You use the AP Radio Hardware pages to assign settings related to the access point's radio hardware. The internal radio and the radio module both have an AP Radio Hardware page. Both pages contain similar settings. Figure 3-11 shows the AP Radio Hardware page for the radio module.

Figure 3-11   The AP Radio Hardware Page for the Radio Module

Follow this link path to reach the AP Radio Hardware pages:

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

2. On the Setup page, click **Hardware** in one of the AP Radio rows under Network Ports.

Settings on the AP Radio Hardware Page

The AP Radio Hardware page contains the following settings:

- Service Set ID (SSID)
- Allow Broadcast SSID to Associate?
- Enable World Mode
- Data Rates
- Transmit Power

- Frag. Threshold
- RTS Threshold
- Max. RTS Retries
- Max. Data Retries
- Beacon Period
- Data Beacon Rate (DTIM)
- Default Radio Channel
- Search for Less-Congested Radio Channel
- Restrict Searched Channels
- Receive Antenna and Transmit Antenna

The AP Radio Hardware page also contains a link to the AP Radio Data Encryption page, which you use to enter Wired Equivalent Privacy (WEP) settings.

Service Set ID (SSID)

The SSID is a 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. The SSID can be any alphanumeric entry up to 32 characters long.

You can also enter this setting on the Express Setup and AP Radio Identification pages.

Allow Broadcast SSID to Associate?

You use this setting to choose whether devices that do not specify an SSID (devices that are "broadcasting" in search of an access point to associate with) are allowed to associate to this radio.

- Yes—This is the default setting; it allows devices that do not specify an SSID (devices that are "broadcasting" in search of an access point to associate with) to associate to this radio.

- No—Devices that do not specify an SSID (devices that are "broadcasting" in search of an access point to associate with) are not allowed to associate to this radio. With no selected, the SSID used by the client device must match exactly the radio's SSID.

Enable World Mode

When you select **yes** from the world-mode pull-down menu, the access point adds channel carrier set information to its beacon. Client devices with world-mode enabled receive the carrier set information and adjust their settings automatically.

Data Rates

You use the data rate settings to choose the data rates the radio uses for data transmission. The rates are expressed in megabits per second.

The access point always attempts to transmit at the highest data rate set to **Basic**. If there are obstacles or interference, the access point steps down to the highest rate that allows data transmission. For each data rate, a drop-down menu lists three options:

- Basic—Allows transmission at this rate for all packets, both unicast and multicast. At least one of the access point's data rates must be set to Basic.

- Yes—The access point transmits only unicast packets at this rate; multicast packets are sent at one of the data rates set to Basic.

- No—The access point does not transmit data at this rate.

You can use the Data Rate settings to set up an access point to serve client devices operating at specific data rates. For example, to set up the internal radio for 11 megabits per second (Mbps) service only, select **Basic** for 11 and select **Yes** for the other data rates. Figure 3-12 shows the Data Rates set up for 11-Mbps service only.

Figure 3-12   Data Rate Settings for 11 Mbps Service Only
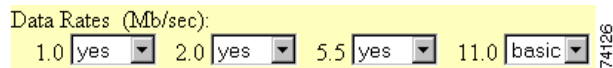
To set up the access point to serve only client devices operating at 1 and 2 Mbps, for example, select **Basic** for 1 and 2 and set the rest of the data rates to **Yes**. Figure 3-13 shows the Data Rates set up for 1- and 2-Mbps service only.

Figure 3-13   Data Rate Settings for 1- and 2-Mbps Service Only

Data Rates (Mb/sec):
1.0 [basic ▼] 2.0 [basic ▼] 5.5 [yes ▼] 11.0 [yes ▼] 74125

The *Optimize Radio Network For* setting on the Express Setup page selects the data rate settings automatically. When you select **Optimize Radio Network For Throughput** on the Express Setup page, all data rates are set to basic. When you select **Optimize Radio Network For Range** on the Express Setup page, the lowest data rate (1.0 on the internal radio and 6.0 on the radio module) is set to basic, and the other data rates are set to yes. If you leave the setting at **Default** for the internal radio, the 1.0 and 5.5 data rates are set to basic and the 2.0 and 11.0 data rates are set to yes (on the radio module, 6.0, 12.0, and 24.0 are set to basic and 9.0, 18.0, 36.0, 48.0, and 54.0 are set to yes).

Transmit Power

This setting determines the power level of radio transmission. The default power setting is the highest transmit power allowed in your regulatory domain.

Note   Government regulations define the highest allowable power level for radio devices. This setting must conform to established standards for the country in which you use the access point.

To reduce interference or to conserve power, select a lower power setting. The settings in the drop-down menu for the internal radio include 1, 5, 20, 50, and 100 milliwatts. The settings in the drop-down menu for the radio module include 5, 8, 11, and 14 milliwatts.

Note   The power settings available on your access point depend on the regulatory domain for which the access point is configured. Your power settings might be different from the settings listed here.

Frag. Threshold

This setting determines the size at which packets are fragmented (sent as several pieces instead of as one block). Enter a setting ranging from 256 to 2338 bytes. Use a low setting in areas where communication is poor or where there is a great deal of radio interference.

RTS Threshold

This setting determines the packet size at which the access point issues a request to send (RTS) before sending the packet. A low RTS Threshold setting can be useful in areas where many client devices are associating with the access point, or in areas where the clients are far apart and can detect only the access point and not each other. Enter a setting ranging from 0 to 2339 bytes.

Max. RTS Retries

The maximum number of times the access point issues an RTS before stopping the attempt to send the packet through the radio. Enter a value from 1 to 128.

Max. Data Retries

The maximum number of attempts the access point makes to send a packet before giving up and dropping the packet.

Beacon Period

The amount of time between beacons in Kilomicroseconds. One Kμsec equals 1,024 microseconds.

Data Beacon Rate (DTIM)

This setting, always a multiple of the beacon period, determines how often the beacon contains a delivery traffic indication message (DTIM). The DTIM tells power-save client devices that a packet is waiting for them.

If the beacon period is set at 100, its default setting, and the data beacon rate is set at 1, its default setting, then the access point sends a beacon containing a DTIM every 100 Kμsecs. One Kμsec equals 1,024 microseconds.

> **Note** If client devices using power-save mode wake up too often when associated to the access point, increase the data beacon rate setting.

Default Radio Channel

The default channel settings on the radios are the lowest channel numbers for your regulatory domain. In North America, the default setting for the internal radio is channel 1 transmitting at 2412 MHz, and the default setting for the radio module is channel 36 transmitting at 5180 MHz. To overcome interference problems, other channel settings are available from the radio channel pull-down menus.

The internal radio operates on 11 channels from 2412 to 2462 MHz. Each channel covers 22 MHz. The bandwidth for channels 1, 6, and 11 does not overlap, so you can set up multiple access points in the same vicinity without causing interference.

The radio module operates on eight channels from 5180 to 5320 MHz. Each channel on the radio module covers 20 MHz, and the bandwidth for the channels overlaps slightly. For best performance, use channels that are not adjacent (44 and 46, for example) for radios that are close to each other.

> **Note** Too many access points in the same vicinity creates radio congestion that can reduce throughput. A careful site survey can determine the best placement of access points for maximum radio coverage and throughput.

Search for Less-Congested Radio Channel

When you select **yes** from the Search for less-congested radio channel pull-down menu, the access point scans for the radio channel that is least busy and selects that channel for use. The access point scans at power-up and when the radio settings are changed.

> **Note** If you need to keep the access point assigned to a specific channel to keep from interfering with other access points, you should leave this setting at **no**.

Restrict Searched Channels

Click **Restrict Searched Channels** to limit the channels that the access point scans when Search for less-congested radio channel is enabled. The AP Radio Restrict Searched Channels page appears when you click Restrict Searched Channels. Figure 3-14 shows the AP Radio Restrict Searched Channels page for the internal radio.

Figure 3-14   AP Radio Restrict Searched Channels Page for the Internal Radio

Channel Number	Frequency (mHz)	Search?
1	2412	☑
2	2417	☑
3	2422	☑
4	2427	☑
5	2432	☑
6	2437	☑
7	2442	☑
8	2447	☑
9	2452	☑
10	2457	☑
11	2462	☑

The page lists all the channels in the access point's regulatory domain. Click the **Search** check boxes beside the channels to include channels in the scan for less-congested channels. All the channels are included in the scan by default.

Receive Antenna and Transmit Antenna

Pull-down menus for the receive and transmit antennas offer three options:

- Diversity—This default setting tells the access point to use the antenna that receives the best signal. If your access point has two fixed (non-removeable) antennas, you should use this setting for both receive and transmit.

- Right—If your access point has removeable antennas and you install a high-gain antenna on the access point's right connector, you should use this setting for both receive and transmit. When you look at the access point's back panel, the right antenna is on the right.

- Left—If your access point has removeable antennas and you install a high-gain antenna on the access point's left connector, you should use this setting for both receive and transmit. When you look at the access point's back panel, the left antenna is on the left.

Note The access point receives and transmits using one antenna at a time, so you cannot increase range by installing high-gain antennas on both connectors and pointing one north and one south. When the access point used the north-pointing antenna, it would ignore client devices to the south.

Entering Advanced Configuration Information

Use the AP Radio Advanced pages to assign special configuration settings for the access point radios. The internal radio and the radio module both have an AP Radio Advanced page. Both pages contain the same settings, but the Advanced page for the external radio module does not contain the Radio Modulation and Radio Preamble settings. Figure 3-15 shows the AP Radio Advanced page for the internal radio.

Figure 3-15   AP Radio Advanced Page for Internal Radio

Follow this link path to reach the AP Radio Advanced pages:

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

2. On the Setup page, click **Advanced** in one of the AP Radio rows under Network Ports.

Settings on the AP Radio Advanced Page

The AP Radio Advanced pages contain the following settings:

- Requested Status
- Packet Forwarding
- Default Multicast Address Filters
- Maximum Multicast Packets/Second
- Radio Cell Role
- Maximum Number of Associations
- Use Aironet Extensions
- Classify Workgroup Bridges as Network Infrastructure
- Require Use of Radio Firmware x.xx
- Ethernet Encapsulation Transform
- Enhanced MIC verification for WEP
- Temporal Key Integrity Protocol
- Broadcast WEP Key rotation interval (sec)
- Accept Authentication Types
- Require EAP
- Default Unicast Address Filter
- Specified Access Points
- Radio Modulation
- Radio Preamble

Requested Status

This setting is useful for troubleshooting problems on your network. Up, the default setting, turns the radio on for normal operation. Down turns the radio off.

The Current Status line under the setting displays the current status of the radio port. This field can also display Error, meaning the port is operating but is in an error condition.

Packet Forwarding

This setting is always set to Enabled for normal operation. For troubleshooting, you might want to set packet forwarding to Disabled, which prevents data from moving between the Ethernet and the radio.

The Forwarding State line under the setting displays the current forwarding state. For normal access point operation, the forwarding state is Forwarding. Four other states are possible:

- Unknown—The state cannot be determined.

- Disabled—Forwarding capabilities are disabled.

- Blocking—The port is blocking transmission. This is the state when no stations are associated.

- Broken—This state reports radio failure.

Default Multicast Address Filters

MAC address filters allow or disallow the forwarding of multicast packets sent to specific MAC addresses. You can create a filter that passes traffic to all MAC addresses except those you specify, or you can create a filter that blocks traffic to all MAC addresses except those you specify. Read the "Creating a MAC Address Filter" section on page 3-15 for complete instructions on setting up MAC address filters.

The pull-down menus for multicast address filters contain two options:

- Allowed—The access point forwards all traffic except packets sent to the MAC addresses listed as disallowed on the Address Filters page.

- Disallowed—The access point discards all traffic except packets sent to the MAC addresses listed as allowed on the Address Filters page.

Note   If you plan to discard traffic to all MAC addresses except those you specify (the Disallowed setting), be sure to enter your own MAC address as allowed on the Address Filters page to prevent being locked out of the access point.

Maximum Multicast Packets/Second

Use this setting to control the number of multicast packets that can pass through the radio port each second. If you enter **0**, the access point passes an unlimited number of multicast packets. If you enter a number other than 0, the device passes only that number of multicast packets per second.

Radio Cell Role

Use this pull-down menu to select the function of the radio within its radio coverage area (cell). This setting determines how the radio interacts with other wireless devices. The menu contains the following options:

- Root—A wireless LAN transceiver that connects an Ethernet network with wireless client stations or with another Ethernet network. Use this setting if the access point is connected to the wired LAN.

- Repeater/Non-Root—A wireless LAN transceiver that transfers data between a client and another access point. Use this setting for access points not connected to the wired LAN.

- Client/Non-root—A station with a wireless connection to an access point. Use this setting for diagnostics or site surveys, such as when you need to test the radio by having it communicate with another access point or bridge without accepting associations from client devices.

Maximum Number of Associations

Use this entry field to specify the maximum number of wireless networking devices that are allowed to associate to the radio. The default setting, 0, means that the maximum possible number of associations is allowed.

Use Aironet Extensions

Select **yes** or **no** to use Cisco Aironet 802.11 extensions. This setting must be set to **yes** (the default setting) to enable these features:

- Load balancing—The access point uses Aironet extensions to direct client devices to an access point that provides the best connection to the network based on factors such as number of users, bit error rates, and signal strength.

- Message Integrity Check (MIC)—MIC is an additional WEP security feature that prevents attacks on encrypted packets called *bit-flip* attacks. The MIC, implemented on both the access point and all associated client devices, adds a few bytes to each packet to make the packets tamper-proof.

- Temporal Key Integrity Protocol (TKIP)—TKIP, also known as WEP key hashing, is an additional WEP security feature that defends against an attack on WEP in which the intruder uses an unencrypted segment called the initialization vector (IV) in encrypted packets to calculate the WEP key.

- Repeater mode—You must set Use Aironet Extensions to yes if the access point is set up as a repeater or if it communicates with a repeater.

The extensions also improve the access point's ability to understand the capabilities of Cisco Aironet client devices associated with the access point.

Classify Workgroup Bridges as Network Infrastructure

Select **no** to allow more than 20 Cisco Aironet Workgroup Bridges to associate to the access point. The default setting, **yes**, limits the number of workgroup bridges that can associate to the access point to 20 or less.

Access points and bridges normally treat workgroup bridges not as client devices but as infrastructure devices, like access points or bridges. Treating a workgroup bridge as an infrastructure device means that the access point reliably delivers multicast packets, including Address Resolution Protocol (ARP) packets, to the workgroup bridge.

The performance cost of reliable multicast delivery—duplication of each multicast packet sent to each workgroup bridge—limits the number of infrastructure devices, including workgroup bridges, that can associate to the access point. To increase beyond 20 the number of workgroup bridges that can associate to the access point, the access point must reduce the delivery reliability of multicast packets to workgroup bridges. With reduced reliability, the access point cannot confirm whether multicast packets reach the intended workgroup

bridge, so workgroup bridges at the edge of the access point's coverage area might lose IP connectivity. When you treat workgroup bridges as client devices, you increase performance but reduce reliability.

> ✎
>
> **Note**   This feature is best suited for use with stationary workgroup bridges. Mobile workgroup bridges might encounter spots in the access point's coverage area where they do not receive multicast packets and lose communication with the access point even though they are still associated to it.

A Cisco Aironet Workgroup Bridge provides a wireless LAN connection for up to eight Ethernet-enabled devices. Refer to the "Overview" section on page 1-2 of the *Cisco Aironet Workgroup Bridge Software Configuration Guide* for a description of workgroup bridges.

Require Use of Radio Firmware x.xx

This setting affects the firmware upgrade process when you load new firmware for the access point. Select **yes** to force the radio firmware to be upgraded to a firmware version compatible with the current version of the management system. Select **no** to exempt the current radio firmware from firmware upgrades.

Ethernet Encapsulation Transform

Choose **802.1H** or **RFC1042** to set the Ethernet encapsulation type. Data packets that are not 802.2 packets must be formatted to 802.2 via 802.1H or RFC1042. Cisco Aironet equipment uses 802.1H because it provides optimum interoperability.

- 802.1H—This default setting provides optimum performance for Cisco Aironet wireless products.
- RFC1042—Use this setting to ensure interoperability with non-Cisco Aironet wireless equipment. RFC1042 does not provide the interoperability advantages of 802.1H but is used by other manufacturers of wireless equipment.

Enhanced MIC verification for WEP

This setting enables Message Integrity Check (MIC), a security feature that protects your WEP keys by preventing attacks on encrypted packets called *bit-flip* attacks. During a bit-flip attack, an intruder intercepts an encrypted message, alters it slightly, and retransmits it, and the receiver accepts the retransmitted message as legitimate. The MIC, implemented on both the access point and all associated client devices, adds a few bytes to each packet to make the packets tamper-proof. Select **MMH** from the pull-down menu and click **Apply** to enable MIC.

> **Note**   MIC takes effect only when the Use Aironet Extensions setting on the AP Radio Advanced page is set to **yes** and WEP is enabled and set to full encryption.

> **Note**   When you enable MIC, only MIC-capable client devices can communicate with the access point.

Temporal Key Integrity Protocol

This setting enables the temporal key integrity protocol (TKIP, also known as WEP key hashing), which defends against an attack on WEP in which the intruder uses the unencrypted initialization vector (IV) in encrypted packets to calculate the WEP key. WEP key hashing removes the predictability that an intruder relies on to determine the WEP key by exploiting IVs. Select **Cisco** from the pull-down menu and click **Apply** to enable WEP key hashing.

> **Note**   To use TKIP, the Use Aironet Extensions setting on the AP Radio Advanced page must be set to **yes** (the default setting).

> **Note**   When you enable TKIP, all WEP-enabled client devices associated to the access point must support WEP key hashing. WEP-enabled devices that do not support TKIP cannot communicate with the access point.

Broadcast WEP Key rotation interval (sec)

This option enables broadcast key rotation by setting a key rotation interval. With broadcast, or multicast, WEP key rotation enabled, the access point provides a dynamic broadcast WEP key and changes it at the interval you select. Broadcast key rotation is an excellent alternative to TKIP if your wireless LAN supports wireless client devices that are not Cisco devices or that cannot be upgraded to the latest firmware for Cisco client devices.

To enable broadcast key rotation, enter the rotation interval in seconds in the Broadcast WEP Key rotation interval entry field. If you enter 900, for example, the access point sends a new broadcast WEP key to all associated client devices every 15 minutes. To disable broadcast WEP key rotation, enter **0**.

> **Note**   When you enable broadcast key rotation, only wireless client devices using LEAP or EAP-TLS authentication can use the access point. Client devices using static WEP (with open, shared key, or EAP-MD5 authentication) cannot use the access point when you enable broadcast key rotation.

> **Note**   If you enable Broadcast Key Rotation on one of the radios in a dual-radio access point, Broadcast Key Rotation is automatically enabled on the other radio, also.

Accept Authentication Types

Select **Open**, **Shared Key**, or **Network-EAP** to set the authentications the access point recognizes. See the "Security Overview" section on page 4-2 for a description of authentication types.

Require EAP

If you use open or shared authentication as well as EAP authentication, select **Require EAP** under Open or Shared to block client devices that are not using EAP from authenticating through the access point.

Default Unicast Address Filter

Unicast MAC address filters allow or disallow the forwarding of unicast packets sent to specific MAC addresses. You can create a filter that passes traffic to all MAC addresses except those you specify, or you can create a filter that blocks traffic to all MAC addresses except those you specify.

Read the "Setting Up MAC-Based Authentication" section on page 4-29 for complete instructions on using MAC-based authentication on an authentication server. Read the "Creating a MAC Address Filter" section on page 3-15 for complete instructions on setting up MAC address filters.

The pull-down menus for unicast address filters contain two options:

- Allowed—The access point forwards all traffic except packets sent to the MAC addresses listed as disallowed on the Address Filters page.

- Disallowed—The access point discards all traffic except packets sent to the MAC addresses listed as allowed on the Address Filters page or on your authentication server.

Select **Disallowed** for each authentication type that also uses MAC-based authentication.

> **Note** If you plan to discard traffic to all MAC addresses except those you specify (the Disallowed setting), be sure to enter your own MAC address as allowed on the Address Filters page or on your authentication server.

Specified Access Points

Use these fields to set up a chain of repeater access points (access points without an Ethernet connection; see Figure 3-3). Repeater access points function best when they associate with specific access points connected to the wired LAN. You use these fields to specify the access points that provide the most efficient data transmission link for the repeater.

If this access point is a repeater, type the MAC address of one or more root-unit access points with which you want this access point to associate. With MAC addresses in these fields, the repeater access point always tries to associate with the specified access points instead of with other less-efficient access points.

If the Adopt Primary Port Identity setting on the specified access point's Radio Identification page is set to **no**, you should enter the radio's MAC address as it appears on the Radio Identification page. Usually, however, the Adopt Primary Port Identity setting is set to **yes**, and you can enter the specified access point's primary MAC address, which appears on the Express Setup page.

For complete instructions on setting up repeater access points, see the "Setting Up a Repeater Access Point" section on page 8-1.

Radio Modulation

Select **Standard** or **MOK** for the radio modulation the access point uses.

- Standard—This default setting is the modulation type specified in IEEE 802.11, the wireless standard published by the Institute of Electrical and Electronics Engineers (IEEE) Standards Association.

- MOK—This modulation was used before the IEEE finished the high-speed 802.11 standard and may still be in use in older wireless networks.

Note This setting does not appear on the AP Radio Advanced page for the radio module.

Radio Preamble

The radio preamble is a section of data at the head of a packet that contains information the access point and client devices need when sending and receiving packets. The pull-down menu allows you to select a long or short radio preamble:

- Long—A long preamble ensures compatibility between the access point and all early models of Cisco Aironet Wireless LAN Adapters (PC4800 and PC4800A).

- Short—A short preamble improves throughput performance. Cisco Aironet's Wireless LAN Adapter supports short preambles. Early models of Cisco Aironet's Wireless LAN Adapter (PC4800 and PC4800A) require long preambles.

Note This setting does not appear on the AP Radio Advanced page for the radio module.

Ethernet Configuration

This section describes how to configure the access point's Ethernet port. You use the Ethernet pages in the management system to set the Ethernet port configuration. The Ethernet pages include:

- Ethernet Identification—Contains the basic locating and identity information for the Ethernet port.

- Ethernet Hardware—Contains the setting for the access point's Ethernet port connection speed.

- Ethernet Advanced—Contains settings for the operational status of the access point's Ethernet port. You can also use this page to make temporary changes in port status to help with troubleshooting network problems.

- Ethernet Port—Lists key information on the access point's Ethernet port.

Entering Identity Information

You use the Ethernet Identification page to enter basic locating and identity information for the access point's Ethernet port. Figure 3-16 shows the Ethernet Identification page.

Figure 3-16   The Ethernet Identification Page

Follow this link path to reach the Ethernet Identification page:

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

2. On the Setup page, click **Identification** in the Ethernet row under Network Ports.

Settings on the Ethernet Identification Page

The Ethernet Identification page contains the following settings:

- Primary Port Settings
- Default IP Address
- Default IP Subnet Mask

The page also displays the access point's MAC address, the system serial number, its current IP address, and its current IP subnet mask.

Primary Port Settings

Two options allow you to designate the access point's Ethernet port as the Primary Port and select whether the Ethernet port adopts or assumes the identity of the primary port.

- Primary Port?—The primary port determines the access point's MAC and IP addresses. Ordinarily, the access point's primary port is the Ethernet port, so this setting is usually set to yes. Select **yes** to set the Ethernet port as the primary port. Select **no** to set the radio port as the primary port.

- Adopt Primary Port Identity?—Select **yes** to adopt the primary port settings (MAC and IP addresses) for the Ethernet port. Select **no** to use different MAC and IP addresses for the Ethernet port.

Some advanced bridge configurations require different settings for the Ethernet and radio ports.

Default IP Address

Use this setting to assign or change the access point's IP address. If DHCP or BOOTP is not enabled for your network, the IP address you enter in this field is the access point's IP address. If DHCP or BOOTP is enabled, this field provides the IP address only if no server responds with an IP address for the access point.

The current IP address displayed under the Default IP Address setting shows the IP address currently assigned to the access point. This is the same address as the default IP address unless DHCP or BOOTP is enabled. If DHCP or BOOTP is enabled, this field displays the IP address that has been dynamically assigned to the device for the duration of its session on the network, and it might be different than the default IP address.

You can also enter this setting on the Express Setup and AP Radio Identification pages.

Default IP Subnet Mask

Enter an IP subnet mask to identify the subnetwork so the IP address can be recognized on the LAN. If DHCP or BOOTP is not enabled, this field is the subnet mask. If DHCP or BOOTP is enabled, this field provides the subnet mask only if no server responds to the access point's request.

The current IP subnet mask displayed under the setting shows the IP subnet mask currently assigned to the access point. This is the same subnet mask as the default subnet mask unless DHCP or BOOTP is enabled. If DHCP or BOOTP is enabled, this is the subnet mask used by the server.

You can also enter this setting on the Express Setup and AP Radio Identification pages.

Entering Ethernet Hardware Information

You use the Ethernet Hardware page to select the connector type, connection speed, and duplex setting used by the access point's Ethernet port. Figure 3-17 shows the Ethernet Hardware page.

Figure 3-17   The Ethernet Hardware Page
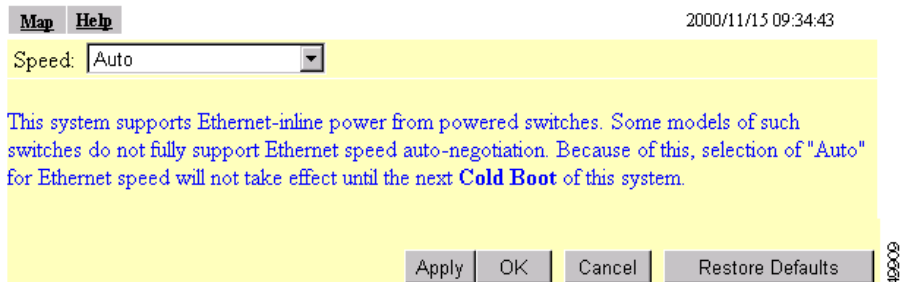
Follow this link path to reach the Ethernet Hardware page:

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

2. On the Setup page, click **Hardware** in the Ethernet row under Network Ports.

Settings on the Ethernet Hardware Page

The Ethernet Hardware page contains one setting:

Speed

The Speed drop-down menu lists five options for the type of connector, connection speed, and duplex setting used by the port. The option you select must match the actual connector type, speed, and duplex settings used to link the port with the wired network.

The default setting, Auto, is best for most networks because the best connection speed and duplex setting are automatically negotiated between the wired LAN and the access point. If you use a setting other than Auto, make sure the hub, switch, or router to which the access point is connected supports your selection.

- Auto—This is the default and the recommended setting. The connection speed and duplex setting are automatically negotiated between the access point and the hub, switch, or router to which the access point is connected.

✎

Note Some switches with inline power do not fully support Ethernet speed auto-negotiation. If your access point is powered by a switch with inline power, the Auto speed setting is applied only after you reboot the access point.

- 10-Base-T / Half Duplex—Ethernet network connector for 10-Mbps transmission speed over twisted-pair wire and operating in half-duplex mode.

- 10-Base-T / Full Duplex—Ethernet network connector for 10-Mbps transmission speed over twisted-pair wire and operating in full-duplex mode.

- 100-Base-T / Half Duplex—Ethernet network connector for 100-Mbps transmission speed over twisted-pair wire and operating in half-duplex mode.

- 100-Base-T / Full Duplex—Ethernet network connector for 100-Mbps transmission speed over twisted-pair wire and operating in full-duplex mode.

Entering Advanced Configuration Information

You use the Ethernet Advanced page to assign special configuration settings for the access point's Ethernet port. Figure 3-18 shows the Ethernet Advanced page.

Figure 3-18   The Ethernet Advanced Page

Follow this link path to reach the Ethernet Advanced page:

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

2. On the Setup page, click **Advanced** in the Ethernet row under Network Ports.

Settings on the Ethernet Advanced Page

The Ethernet Advanced page contains the following settings:

- Requested Status
- Packet Forwarding
- Default Unicast and Multicast Address Filters
- Maximum Multicast Packets/Second

Requested Status

This setting is useful for troubleshooting problems on your network. Up, the default setting, enables the Ethernet port for normal operation. Down disables the access point's Ethernet port.

The Current Status line under the setting displays the current status of the Ethernet port. This field can also display Error, meaning the port is in an error condition.

Packet Forwarding

This setting is always set to Enabled for normal operation. For troubleshooting, you might want to set packet forwarding to Disabled, which prevents data from moving between the Ethernet and the radio.

The Forwarding State line under the setting displays the current forwarding state. The state for normal operation is Forwarding. Four other settings are possible:

- Unknown—The state cannot be determined.

- Disabled—Forwarding capabilities are disabled.

- Blocking—The port is blocking transmission.

- Broken—This state reports an Ethernet port failure.

Default Unicast and Multicast Address Filters

MAC address filters allow or disallow the forwarding of unicast and multicast packets sent to specific MAC addresses. You can create a filter that passes traffic to all MAC addresses except those you specify, or you can create a filter that blocks traffic to all MAC addresses except those you specify. Read the "Creating a MAC Address Filter" section on page 3-15 for complete instructions on setting up MAC address filters.

Unicast packets are addressed to just one device on the network. *Multicast* packets are addressed to multiple devices on the network.

The pull-down menus for unicast and multicast address filters contain two options:

- Allowed—The access point forwards all traffic except packets sent to the MAC addresses listed as disallowed on the Address Filters page.

- Disallowed—The access point discards all traffic except packets sent to the MAC addresses listed as allowed on the Address Filters page.

> **Note** For most configurations, you should leave Default Multicast Address Filter set to
> **Allowed**. If you intend to set it to **Disallowed**, add the broadcast MAC address
> (ffffffffffff) to the list of allowed addresses on the Address Filters page before
> changing the setting to prevent being locked out of the access point.

> **Note** If you plan to discard traffic to all MAC addresses except those you specify (the
> Disallowed setting), be sure to enter your own MAC address as allowed on the
> Address Filters page to prevent being locked out of the access point.

Maximum Multicast Packets/Second

Use this setting to control the number of multicast packets that can pass through
the Ethernet port each second. If you enter **0**, the access point passes an unlimited
number of multicast packets. If you enter a number other than 0, the device passes
only that number of multicast packets per second.

Server Setup

This section describes how to configure the server to support access point
features. You use separate management system pages to enter server settings. The
server setup pages are described in the following sections:

- Entering Time Server Settings, page 3-49
- Entering Boot Server Settings, page 3-51
- Entering Web Server Settings and Setting Up Access Point Help, page 3-55
- Entering Name Server Settings, page 3-58
- Entering FTP Settings, page 3-60

> **Note** See the "Enabling EAP on the Access Point" section on page 4-20 for instructions
> on setting up the authentication server.

Entering Time Server Settings

You use the Time Server Setup page to enter time server settings. Figure 3-19 shows the Time Server Setup page:

Figure 3-19   Time Server Setup Page

Follow this link path to reach the Time Server Setup page:

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

2. On the Setup page, click **Time Server** under Services.

Settings on the Time Server Setup Page

The Time Server Setup page contains the following settings:

- Simple Network Time Protocol
- Default Time Server
- GMT Offset (hr)
- Use Daylight Savings Time
- Manually Set Date and Time

Simple Network Time Protocol

Select **Enabled** or **Disabled** to turn Simple Network Time Protocol (SNTP) on or off. If your network uses SNTP, select **Enabled**.

Default Time Server

If your network has a default time server, enter the server's IP address in the Default Time Server entry field.

The Current Time Server line under the entry field reports the time server the access point is currently using.

> **Note**   The DHCP or BOOTP server can override the default time server.

GMT Offset (hr)

The GMT Offset pull-down menu lists the world's time zones relative to Greenwich Mean Time (GMT). Select the time zone in which the access point operates.

Use Daylight Savings Time

Select **yes** or **no** to have the access point automatically adjust to Daylight Savings Time.

Manually Set Date and Time

Enter the current date and time in the entry fields to override the time server or to set the date and time if no server is available.

When entering the date and time, use forward-slashes to separate the year, month, and day, and use colons to separate the hours, minutes, and seconds. For example, you would enter 2001/02/17 for February 17, 2001, and 18:25:00 for 6:25 pm.

Entering Boot Server Settings

You use the Boot Server Setup page to configure the access point for your network's BOOTP or DHCP servers for automatic assignment of IP addresses. Figure 3-20 shows the Boot Server Setup page:

Figure 3-20   Boot Server Setup Page

Follow this link path to reach the Boot Server Setup page:

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

2. On the Setup page, click **Boot Server** under Services.

Settings on the Boot Server Setup Page

The Boot Server Setup page contains the following settings:

- Configuration Server Protocol
- Use Previous Configuration Server Settings

- Read .ini File from File Server
- BOOTP Server Timeout (sec)
- DHCP Multiple-Offer Timeout (sec)
- DHCP Requested Lease Duration (min)
- DHCP Minimum Lease Duration (min)
- DHCP Client Identifier Type
- DHCP Client Identifier Value
- DHCP Class Identifier

Configuration Server Protocol

Use the Configuration Server Protocol pull-down menu to select your network's method of IP address assignment. The menu contains the following options:

- None—Your network does not have an automatic system for IP address assignment.
- BOOTP—Your network uses Boot Protocol, in which IP addresses are hard-coded based on MAC addresses.
- DHCP—With Dynamic Host Configuration Protocol, IP addresses are leased for a period of time. You can set the lease duration with the settings on this page.

Use Previous Configuration Server Settings

Select **yes** to have the access point save the boot server's most recent response. The access point uses the most recent settings if the boot server is unavailable.

Read .ini File from File Server

Use this setting to have the access point use configuration settings in an .ini file on the BOOTP or DHCP server or the default file server. Files with .ini extensions usually contain configuration information used during system start-up. The pull-down menu contains the following options:

- Always—The access point always loads configuration settings from an .ini file on the server.

- Never—The access point never loads configuration settings from an .ini file on the server.

- If specified by server—The access point loads configuration settings from an .ini file on the server if the server's DHCP or BOOTP response specifies that an .ini file is available. This is the default setting.

The Load Now button under the pull-down menu tells the access point to read an .ini file immediately.

The Current Boot Server line under the pull-down menu lists the server that responded to the access point's boot request. If all zeros appear, it means that the access point is not using BOOTP/DHCP or that no server responded to the BOOTP/DHCP request. The Specified ".ini" File Server line lists the IP address of the server where the .ini file is stored. If all zeroes appear, it means that no file server is set up to provide an .ini file.

BOOTP Server Timeout (sec)

This setting specifies the length of time the access point waits to receive a response from a single BOOTP server. Enter the number of seconds the access point should wait. This setting applies only when you select BOOTP from the Configuration Server Protocol pull-down menu.

DHCP Multiple-Offer Timeout (sec)

This setting specifies the length of time the access point waits to receive a response when there are multiple DHCP servers. Enter the number of seconds the access point should wait.

DHCP Requested Lease Duration (min)

This setting specifies the length of time the access point requests for an IP address lease from your DHCP server. Enter the number of minutes the access point should request.

DHCP Minimum Lease Duration (min)

This setting specifies the shortest amount of time the access point accepts for an IP address lease. The access point ignores leases shorter than this period. Enter the minimum number of minutes the access point should accept for a lease period.

DHCP Client Identifier Type

Use this optional setting to include a class identifier type in the DHCP request packets the access point sends to your DHCP server. Your DHCP server can be set up to send responses according to class identifier type. If most of the client devices using the access point are the same device type, you can select that device type to be included in the DHCP request packet.

Use **Ethernet (10Mb)**, the default setting, if you do not intend to set up your DHCP server to send responses according to class identifier type.

If you want to include a unique value in the DHCP Client Identifier Value field (the setting under DHCP Client Identifier Type on the Boot Server Setup page), select **Other - Non Hardware**.

Table 3-1 lists the options in the DHCP Client Identifier Type pull-down menu.

Table 3-1   Options in the DHCP Client Identifier Type Menu

Option	Definition
Ethernet (10Mb)	This is the default setting. Use this setting if you do not need your DHCP server to send responses based on the class identifier in the access point's DHCP request packets.
Experimental Ethernet	Select one of these specific device types if most of the client devices using the access point are the same device type. The access point includes the device type in the DHCP request packets it sends to the DHCP server.
Amateur Radio AX.25	
Proteon ProNET Token Ring	
Chaos	
IEEE 802 Networks	
ARCNET	
Hyperchannel	
Lanstar	
Autonet Short Address	
LocalTalk	
LocalNet	
Other - Non Hardware	Select this option to include a unique value in the DHCP Client Identifier Value field.

DHCP Client Identifier Value

Use this setting to include a unique identifier in the access point's DHCP request packet. This field contains the access point's MAC address by default. If you select **Other - Non Hardware** from the DHCP Client Identifier Type pull-down menu, you can enter up to 255 alphanumeric characters. If you select any other option from the DHCP Client Identifier Type pull-down menu, you can enter up to 12 hexadecimal characters. Hexadecimal characters include the numbers 0 through 9 and the letters A through F.

DHCP Class Identifier

Your DHCP server can be set up to send responses according to the group to which a device belongs. Use this field to enter the access point's group name. The DHCP server uses the group name to determine the response to send to the access point. The access point's DHCP class identifier is a vendor class identifier.

Entering Web Server Settings and Setting Up Access Point Help

You use the Web Server Setup page to enable browsing to the web-based management system, specify the location of the access point Help files, and enter settings for a custom-tailored web system for access point management. Figure 3-21 shows the Web Server Setup page:

Figure 3-21   Web Server Setup Page

Follow this link path to reach the Web Server Setup page:

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

2. On the Setup page, click **Web Server** under Services.

Settings on the Web Server Setup Page

The Web Server Setup page contains the following settings:

- Allow Non-Console Browsing
- HTTP Port
- Default Help Root URL
- Extra Web Page File
- Default Web Root URL

Allow Non-Console Browsing

Select **yes** to allow browsing to the management system. If you select no, the management system is accessible only through the console and Telnet interfaces.

HTTP Port

This setting determines the port through which your access point provides web access. Your System Administrator should be able to recommend a port setting.

Default Help Root URL

This entry tells the access point where to look for the Help files. The Help button on each management system page opens a new browser window displaying help for that page. You can point to the help files in one of three possible locations:

- Internet—Cisco maintains up-to-date help for access points on the Cisco website. While this location requires online access for every occasion of needing online help, it offers the most up-to-date information. If you use this help location, which is the default setting, you don't need to copy the files from the access point and bridge CD.

- File Server—On multi-user networks, the help files can be placed on the network file server. For this location, enter the full directory URL in the Default Help Root URL entry field. Your entry might look like this:

  [system name]\[directory]\wireless\help

- Hard Drive—you can copy the help files to the hard drive of the computer you use to manage the wireless LAN. If you use this location, enter the full directory URL. Your entry might look like this:

  file:///[drive letter]:\[folder or subdirectory]\wireless\help

Extra Web Page File

If you need to create an alternative to the access point's management system, you can create HTML pages and load them into the access point. You use this entry field to specify the filename for your HTML page stored on the file server.

Click **Load Now** to load the HTML page.

Default Web Root URL

This setting points to the access point management system's HTML pages. If you create alternative HTML pages, you should change this setting to point to the alternative pages. The default setting is:

mfs0:/StdUI/

Entering Name Server Settings

You use the Name Server Setup page to configure the access point to work with your network's Domain Name System (DNS) server. Figure 3-22 shows the Name Server Setup page:

Figure 3-22   The Name Server Setup Page

Follow this link path to reach the Name Server Setup page:

- On the Summary Status page, click **Setup**
- On the Setup page, click **Name Server** under Services.

Settings on the Name Server Setup Page

The Name Server Setup page contains the following settings:

- Domain Name System
- Default Domain
- Domain Name Servers
- Domain Suffix

Domain Name System

If your network uses a Domain Name System (DNS), select **Enabled** to direct the access point to use the system. If your network does not use DNS, select **Disabled**.

Default Domain

Enter the name of your network's IP domain in the entry field. Your entry might look like this:

mycompany.com

The Current Domain line under the entry field lists the domain that is serving the access point. The current domain might be different from the domain in the entry field if, on the Boot Server Setup page, you have DHCP or BOOTP set as the Configuration Server Protocol, but you selected No for the setting "Use previous Configuration Server settings when no server responds?"

Domain Name Servers

Enter the IP addresses of up to three domain name servers on your network. The Current lines to the right of the entry fields list the servers the access point is currently using, which may be specified by the DHCP or BOOTP server.

Domain Suffix

In this entry field, enter the portion of the full domain name that you would like omitted from access point displays. For example, in the domain "mycompany.com" the full name of a computer might be "mycomputer.mycompany.com." With domain suffix set to "mycompany.com," the computer's name would be displayed on management system pages as simply "mycomputer."

Entering FTP Settings

You use the FTP Setup page to assign File Transfer Protocol settings for the access point. All non-browser file transfers are governed by the settings on this page. Figure 3-23 shows the FTP Setup page:

Figure 3-23   The FTP Setup Page

Follow this link path to reach the FTP Setup page:

- On the Summary Status page, click **Setup**
- On the Setup page, click **FTP** under Services.

Settings on the FTP Setup Page

The FTP Setup page contains the following settings:

- File Transfer Protocol
- Default File Server
- FTP Directory
- FTP User Name
- FTP User Password

File Transfer Protocol

Use the pull-down menu to select **FTP** or **TFTP** (Trivial File Transfer Protocol). TFTP is a relatively slow, low-security protocol that requires no username or password.

Default File Server

Enter the IP address or DNS name of the file server where the access point should look for FTP files.

FTP Directory

Enter the file server directory that contains the firmware image files.

FTP User Name

Enter the username assigned to your FTP server. You don't need to enter a name in this field if you select TFTP as the file transfer protocol.

FTP User Password

Enter the password associated with the file server's username. You don't need to enter a password in this field if you select TFTP as the file transfer protocol.

Routing Setup

You use the Routing Setup page to configure the access point to communicate with the IP network routing system. You use the page settings to specify the default gateway and to build a list of installed network route settings. Figure 3-24 shows the Routing Setup page.

Figure 3-24   Routing Setup Page

Follow this link path to reach the Routing Setup page:

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

2. On the Setup page, click **Routing** under Services.

Entering Routing Settings

The Routing Setup page contains the following settings:

- Default Gateway
- New Network Route Settings
- Installed Network Routes list

Default Gateway

Enter the IP address of your network's default gateway in this entry field. The entry 255.255.255.255 indicates no gateway.

New Network Route Settings

You can define additional network routes for the access point. To add a route to the installed list, fill in the three entry fields and click **Add**. To remove a route from the list, highlight the route and click **Remove**. The three entry fields include:

- Dest Network—Enter the IP address of the destination network.

- Gateway—Enter the IP address of the gateway used to reach the destination network.

- Subnet Mask—Enter the subnet mask associated with the destination network.

Installed Network Routes list

The list of installed routes provides the destination network IP address, the gateway, and the subnet mask for each installed route.

Association Table Display Setup

You use the Association Table Filters and the Association Table Advanced pages to customize the display of information in the access point's Association Table.

Association Table Filters Page

Figure 3-25 shows the Association Table Filters page.

Figure 3-25   Association Table Filters Page

Follow this link path to reach the Association Table Filters page:

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

2. On the Setup page, click **Display Defaults** under Associations.

You can also reach the Association Table Filters page through the "additional display filters" link on the Association Table page. When you reach the page through the "additional display filters" link, four buttons appear at the bottom of the page that are different from the standard buttons on management system pages. The buttons include:

- Apply—Applies your selections to the Association Table and returns you to the Association Table page.

- Save as Default—Saves your selections as new default settings and returns you to the Association Table page.

- Restore Current Defaults—Applies the currently saved default settings to the Association Table and returns you to the Association Table page.

- Restore Factory Defaults—Applies the factory default settings to the Association Table and returns you to the Association Table page.

Settings on the Association Table Filters Page

The Association Table Filters page contains the following settings:

- Stations to Show
- Fields to Show
- Packets To/From Station
- Bytes To/From Station
- Primary Sort
- Secondary Sort

Stations to Show

Select the station types that you want to be displayed in the Association Table. If you select all station types, all stations of these types appear in the access point's Association Table.

Fields to Show

The fields you select here are the column headings for the Association Table. Fields include:

- System Name—A device's system name.

- State—A device's operational state. Possible states include:
    - Assoc—The station is associated with an access point.
    - Unauth—The station is unauthenticated with any access point.
    - Auth—The station is authenticated with an access point.

- IP Address—A device's IP address.

- Parent—A wireless client device's parent device, which is usually an access point.

- Device—A device's type, such as a 350 series access point or a PC Client Card. Non-Aironet devices appear as "Generic 802.11" devices.

- SW Version—The current version of firmware on a device.

- Class—A device's role in the wireless LAN. Classes include:

  – AP—an access point station.

  – Client or PS Client—a client or power-save client station.

  – Bridge, Bridge R—a bridge or a root bridge.

  – Rptr—a repeater access point.

  – Mcast—a multicast address.

  – Infra—an infrastructure node, usually a workstation with a wired connection to the Ethernet network.

Packets To/From Station

Use these settings to display packet volume information in the Association Table. Select **Total** to display the total number of packets to and from each station on the network.

Select **Alert** to display the number of alert packets to and from each station on the network for which you have activated alert monitoring. Select the **Alert** checkbox on a device's Station page to activate alert monitoring for that device. See the "Using Station Pages" section on page 5-3 for details on Station pages.

The Total and Alert selections both add a column to the Association Table.

Bytes To/From Station

Use these settings to display byte volume information in the Association Table. Select **Total** to display the total number of bytes to and from each station on your wireless network. Select **Alert** to display the number of alert bytes to and from each station on the wireless network. Both selections add a column to the Association Table.

Primary Sort

This setting determines the information that appears in the first column in the Association Table.

Secondary Sort

This setting determines the information that appears in the second column in the Association Table.

Association Table Advanced Page

You use the Association Table Advanced page to control the total number of devices the access point can list in the Association Table and the amount of time the access point continues to track each device class when a device is inactive. Figure 3-26 shows the Association Table Advanced page.

Figure 3-26   Association Table Advanced Page

Follow this link path to reach the Association Table Advanced page:

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

2. On the Setup page, click **Advanced** under Associations.

Settings on the Association Table Advanced Page

The Association Table Advanced page contains the following settings:

- Handle Station Alerts as Severity Level
- Maximum number of bytes stored per Station Alert packet
- Maximum Number of Forwarding Table Entries
- Aironet Extended Statistics in MIB (awcTpFdbTable)
- Block ALL Inter-Client Communications (PSPF)
- Default Activity Timeout (seconds) Per Device Class

Handle Station Alerts as Severity Level

This setting determines the Severity Level at which Station Alerts are reported in the Event Log. This setting also appears on the Event Handling Setup page. You can choose from four Severity Levels:

- Fatal Severity Level (System, Protocol, Port)— Fatal-level events indicate an event that prevents operation of the port or device. For operation to resume, the port or device usually must be reset. Fatal-level events appear in red in the Event Log.

- Alert Severity Level (System, Protocol, Port, External)—Alert-level messages indicate that you need to take action to correct the condition and appear in magenta in the Event Log.

- Warning Severity Level (System, Protocol, Port, External)—Warning-level messages indicate that an error or failure may have occurred and appear in blue in the Event Log.

- Information Severity Level (System, Protocol, Port, External)—Information-level messages notify you of some sort of event, not fatal (that is, the port has been turned off, the rate setting has been changed, etc.) and appear in green in the Event Log.

Maximum number of bytes stored per Station Alert packet

This setting determines the maximum number of bytes the access point stores for each Station Alert packet when packet tracing is enabled. If you use 0 (the default setting), the access point does not store bytes for Station Alert packets; it only logs the event. See the "Event Handling Setup Page" section on page 3-74 for instructions on enabling packet tracing.

Maximum Number of Forwarding Table Entries

This setting determines the maximum number of devices that can appear in the Association Table.

Aironet Extended Statistics in MIB (awcTpFdbTable)

Use this setting to enable or disable the storage of detailed statistics in access point memory. When you disable extended statistics you conserve memory, and the access point can include more devices in the Association Table.

Block ALL Inter-Client Communications (PSPF)

Publicly Secure Packet Forwarding (PSPF) prevents client devices associated to an access point from inadvertently sharing files with other client devices on the wireless network. It provides Internet access to client devices without providing other capabilities of a LAN. With PSPF enabled, client devices cannot communicate with other client devices on the wireless network. This feature is useful for public wireless networks like those installed in airports or on college campuses.

Default Activity Timeout (seconds) Per Device Class

These settings determine the number of seconds the access point continues to track an inactive device depending on its class. A setting of zero tells the access point to track a device indefinitely no matter how long it is inactive. A setting of 300 equals 5 minutes; 1800 equals 30 minutes; 28800 equals 8 hours.

Event Notification Setup

You use the Event Display Setup, Event Handling Setup, and Event Notifications Setup pages to customize the display of access point events (alerts, warnings, and normal activity).

Event Display Setup Page

You use the Event Display Setup page to determine how time should be displayed on the Event Log. In addition, you can determine what severity level is significant enough to display an event. Figure 3-27 shows the Event Display Setup page.

Figure 3-27   The Event Display Setup Page

Follow this link path to reach the Event Display Setup page:

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

2. On the Setup page, click **Display Defaults** under Event Log.

Settings on the Event Display Setup Page

The Event Display Setup page contains the following settings:

- How should time generally be displayed?
- How should Event Elapsed (non-wall-clock) Time be displayed?
- Severity Level at which to display events

How should time generally be displayed?

You use this pull-down menu to determine whether the events in the Event Log are displayed as system uptime or wall-clock time. If you select system uptime, the events are displayed either since the boot or since the last time the Event Log was displayed. If you select wall-clock time, the events are displayed in a YY:MM:DD HH:MM:SS format. If time has not been set on the access point (either manually or by a time server), the time display appears as uptime regardless of this selection.

How should Event Elapsed (non-wall-clock) Time be displayed?

Choose to display event time since the last boot-up of the access point or the time that has elapsed since the event occurred.

Severity Level at which to display events

When an event occurs, it may be displayed immediately on the console, on the console log, or on the GUI log for read purposes only. The event may also be recorded. (You control display and recording of events through the Event Handling Setup page; see the "Event Handling Setup Page" section on page 3-74 for details.) Use the pull-down menus to choose one of the sixteen severity levels for each display area. Table 3-2 lists the severity levels.

Table 3-2   Event Display Severity Levels

Severity Level	Description
silent	The *silent* setting directs the access point to not display any events immediately on the console, the console log, or the GUI log.
System Fatal Protocol Fatal Port Fatal	The Fatal settings indicate an event that prevents operation of the port or device. For operation to resume, the port or device usually must be reset. • System refers to the access point as a whole. • Protocol refers to a specific communications protocol in use, such as HTTP or IP. • Port refers to the access point's Ethernet or radio network interface.
System alert Protocol alert Port alert External alert	The Alert settings indicate events of which an administrator specifically requested to be informed. • System refers to the access point as a whole. • Protocol refers to a specific communications protocol in use, such as HTTP or IP. • Port refers to the access point's Ethernet or radio network interface. • External refers to a device on the network other than the access point.

Table 3-2   Event Display Severity Levels (continued)

Severity Level	Description
System warning Protocol warning Port warning External warning	The Warning settings indicate that a failure has occurred. • System refers to the access point as a whole. • Protocol refers to a specific communications protocol in use, such as HTTP or IP. • Port refers to the access point's Ethernet or radio network interface. • External refers to a device on the network other than the access point.
System information Protocol information Port information External information	The Information settings indicate a normal action that isn't fatal (that is, the port has been turned off, the rate setting has been changed, etc.) • System refers to the access point as a whole. • Protocol refers to a specific communications protocol in use, such as HTTP or IP. • Port refers to the access point's Ethernet or radio network interface. • External refers to a device on the network other than the access point.

These selections affect display of events only. They are used to filter information, not to remove it from the Event Log. To remove information from the Event Log, click **Purge Log** on the Event Log page.

Event Handling Setup Page

You use the Event Handling Setup page to determine how notification of the fatal, alert, warning, and information events should occur. You can choose to only count the events, display them to the console but not store them, record them after

displaying them on the console, or notify someone of the occurrence after displaying and recording the event. Figure 3-28 shows the Event Handling Setup page.

Figure 3-28   The Event Handling Setup Page

Follow this link path to reach the Event Handling Setup page:

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

2. On the Setup page, click **Event Handling** under Event Log.

Settings on the Event Handling Setup Page

The Event Handling Setup page contains the following settings:

- Disposition of Events
- Handle Station Events as Severity Level
- Maximum memory reserved for Detailed Event Trace Buffer (bytes)
- Download Detailed Event Trace Buffer
- Clear Alert Statistics
- Purge Trace Buffer

Disposition of Events

The event settings control how events are handled by the access point: counted, displayed in the log, recorded, or announced in a notification. The settings are color coded: red for fatal errors, magenta for alerts, blue for warnings, and green for information. You select an option from each setting's pull-down menu. Each option includes and builds upon the previous option.

- Count—Tallies the total events occurring in this category without any form of notification or display.
- Display Console—Provides a read-only display of the event but does not record it.
- Record—Makes a record of the event in the log and provides a read-only display of the event.
- Notify—Makes a record of the event in the log, displays the event, and tells the access point to notify someone of the occurrence.

Handle Station Events as Severity Level

You use this setting to set a severity level for Station Alerts. Use the pull-down menu to choose one of the sixteen severity levels. Table 3-2 on page 3-73 lists the severity levels in the menu. The *silent* option is not available for station events, however.

Maximum memory reserved for Detailed Event Trace Buffer (bytes)

Enter the number of bytes reserved for the Detailed Event Trace Buffer. The Detailed Event Trace Buffer is a tool for tracing the contents of packets between specified stations on your network.

After you reserve space for the trace buffer, browse to a device's Station page and select the **Alert** checkboxes in the To Station and From Station columns. See the "Browsing to Network Devices" section on page 5-2 for instructions on opening a device's Station page.

Download Detailed Event Trace Buffer

Use these links to view Headers Only or All Data in the detailed trace buffer. The number of bytes saved per packet is controlled on the Association Table Advanced Setup page.

If your browser is Netscape Communicator, click the links with your left mouse button to view the trace data. Click the links with your right mouse button and select **Save Link As** to save the data in a file.

Clear Alert Statistics

Click this button to reset the alert tallies to 0.

Purge Trace Buffer

Click this button to delete the packet traces from the Event Trace Buffer.

Event Notifications Setup Page

You use the Event Notifications Setup page to enable and configure notification of fatal, alert, warning, and information events to destinations external to the access point, such as an SNMP server or a Syslog system.

✎

Note For event notifications to be sent to an external destination, the events must be set to Notify on the Event Handling Setup page. See the "Event Handling Setup Page" section on page 3-74 for a description of the settings on the Event Handling Setup page.

Figure 3-29 shows the Event Notifications Setup page.

Figure 3-29   Event Notifications Setup Page

Follow this link path to reach the Event Notifications Setup page:

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

2. On the Setup page, click **Event Notifications** under Event Log.

Settings on the Event Notifications Setup Page

The Event Notifications Setup page contains the following settings:

- Should Notify-Disposition Events generate SNMP Traps?
- SNMP Trap Destination
- SNMP Trap Community
- Should Notify-Disposition Events generate Syslog Messages?
- Syslog Destination Address
- Syslog Facility Number

Should Notify-Disposition Events generate SNMP Traps?

Select **yes** to send event notifications to an SNMP server.

![Note icon]

Note   For notifications to be sent to an SNMP server, SNMP must be enabled on the SNMP Setup page, and you must set an SNMP trap destination and an SNMP trap community.

SNMP Trap Destination

Type the IP address or the host name of the server running the SNMP Management software. This setting also appears on the SNMP Setup page.

SNMP Trap Community

Type the SNMP community name. This setting also appears on the SNMP Setup page.

Should Notify-Disposition Events generate Syslog Messages?

Select yes to send event notifications to a Syslog server.

Syslog Destination Address

Type the IP address or the host name of the server running Syslog.

The Network Default Syslog Destination line under the syslog destination address field lists the syslog destination address provided by the DHCP or BOOTP server. This default syslog destination is only used if the syslog destination address field is blank.

Syslog Facility Number

Type the Syslog Facility number for the notifications. The default setting is 16, which corresponds to the Local0 facility code.

Security Setup

This chapter describes how to set up your access point's security features. This chapter contains the following sections:

Security Overview

This section describes the types of security features you can enable on the access point. The security features protect wireless communication between the access point and other wireless devices, control access to your network, and prevent unauthorized entry to the access point management system.

On an access point with two radios, you can assign different security settings to each radio.

Levels of Security

Security is vital for any wireless network, and you should enable all the security features available on your network. Figure 4-1 shows possible levels of security on Cisco Aironet wireless networking equipment, from no security on the left to highest security on the right. The highest level of security, EAP authentication, interacts with a Remote Authentication Dial-In User Service (RADIUS) server on your network to provide authentication service for wireless client devices.

Figure 4-1   Wireless LAN Security Levels
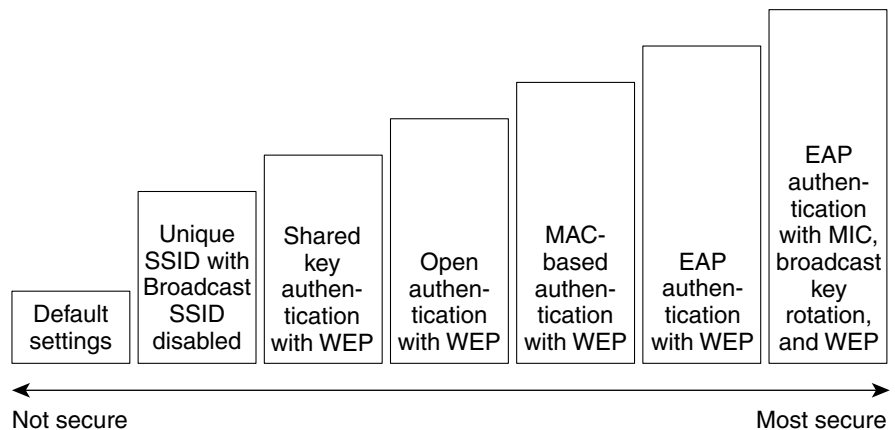
If you don't enable any security features on your access point, anyone with a wireless networking device is able to join your network. If you enable open or shared-key authentication with WEP encryption, your network is safe from casual outsiders but vulnerable to intruders who use a hacking algorithm to calculate the WEP key. If you enable server-based EAP authentication with Message Integrity Check (MIC), Temporal Key Integrity Protocol (TKIP, also known as key hashing), and broadcast key rotation, your network is safe from all but the most sophisticated attacks against wireless security.

Encrypting Radio Signals with WEP

Just as anyone within range of a radio station can tune to the station's frequency and listen to the signal, any wireless networking device within range of an access point can receive the access point's radio transmissions. Because WEP (Wired Equivalent Privacy) is the first line of defense against intruders, Cisco recommends that you use full encryption on your wireless network.

WEP encryption scrambles the communication between the access point and client devices to keep the communication private. Both the access point and client devices use the same WEP key to encrypt and unencrypt radio signals. WEP keys encrypt both unicast and multicast messages. Unicast messages are addressed to just one device on the network. Multicast messages are addressed to multiple devices on the network.

Extensible Authentication Protocol (EAP) authentication provides dynamic WEP keys to wireless users. Dynamic WEP keys are more secure than static, or unchanging, WEP keys. If an intruder passively receives enough packets encrypted by the same WEP key, the intruder can perform a calculation to learn the key and use it to join your network. Because they change frequently, dynamic WEP keys prevent intruders from performing the calculation and learning the key.

Additional WEP Security Features

Three additional security features defend your wireless network's WEP keys:

- Message Integrity Check (MIC)—MIC prevents attacks on encrypted packets called *bit-flip* attacks. During a bit-flip attack, an intruder intercepts an encrypted message, alters it slightly, and retransmits it, and the receiver accepts the retransmitted message as legitimate. The MIC, implemented on

both the access point and all associated client devices, adds a few bytes to each packet to make the packets tamper-proof. See the "Enabling Message Integrity Check (MIC)" section on page 4-14 for instructions on enabling MIC.

- TKIP (Temporal Key Integrity Protocol, also known as WEP key hashing)—This feature defends against an attack on WEP in which the intruder uses the unencrypted initialization vector (IV) in encrypted packets to calculate the WEP key. TKIP removes the predictability that an intruder relies on to determine the WEP key by exploiting IVs. See the "Enabling Temporal Key Integrity Protocol (TKIP)" section on page 4-16 for instructions on enabling TKIP.

- Broadcast key rotation—EAP authentication provides dynamic unicast WEP keys for client devices but uses static broadcast, or multicast, keys. When you enable broadcast WEP key rotation, the access point provides a dynamic broadcast WEP key and changes it at the interval you select. Broadcast key rotation is an excellent alternative to TKIP if your wireless LAN supports wireless client devices that are not Cisco devices or that cannot be upgraded to the latest firmware for Cisco client devices. See the "Enabling Broadcast WEP Key Rotation" section on page 4-18 for instructions on enabling broadcast key rotation.

Network Authentication Types

Before a wireless client device can communicate on your network through the access point, it must authenticate to the access point and to your network. The access point uses four authentication mechanisms or types and can use more than one at the same time:

- Network-EAP—This authentication type provides the highest level of security for your wireless network. By using the Extensible Authentication Protocol (EAP) to interact with an EAP-compatible RADIUS server, the access point helps a wireless client device and the RADIUS server to perform mutual authentication and derive a dynamic unicast WEP key. The RADIUS server sends the WEP key to the access point, which uses it for all unicast data signals that it sends to or receives from the client. The access point also encrypts its broadcast WEP key (entered in the access point's WEP key slot 1) with the client's unicast key and sends it to the client.

When you enable EAP on your access points and client devices, authentication to the network occurs in the steps shown in Figure 4-2:

Figure 4-2   Sequence for EAP Authentication
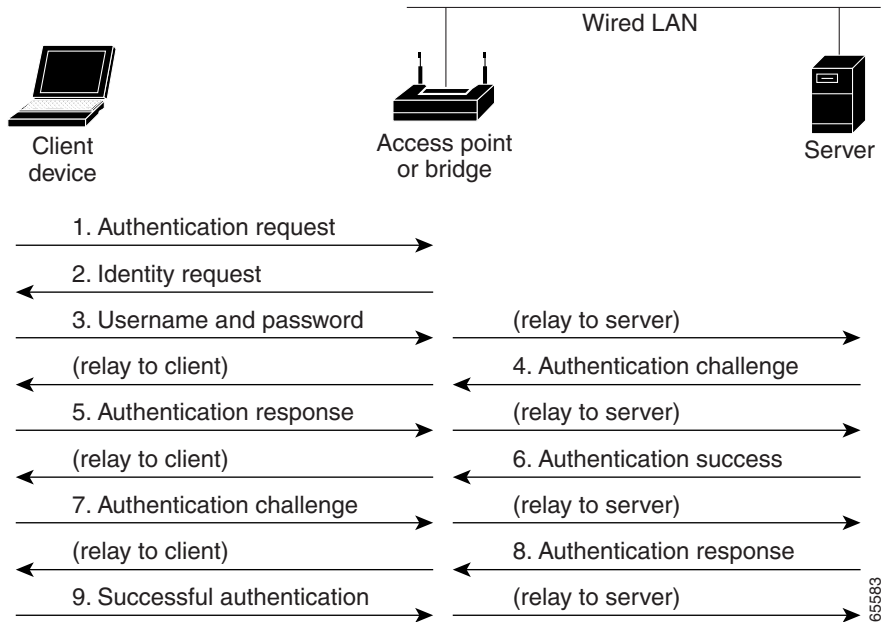
In steps 1 through 9 in Figure 4-2, a wireless client device and a RADIUS server on the wired LAN use 802.1x and EAP to perform a mutual authentication through the access point. The RADIUS server sends an authentication challenge to the client. The client uses a one-way encryption of the user-supplied password to generate a response to the challenge and sends that response to the RADIUS server. Using information from its user database, the RADIUS server creates its own response and compares that to the response from the client. When the RADIUS server authenticates the client, the process repeats in reverse, and the client authenticates the RADIUS server.

When mutual authentication is complete, the RADIUS server and the client determine a WEP key that is unique to the client and provides the client with the appropriate level of network access, thereby approximating the level of security in a wired switched segment to an individual desktop. The client loads this key and prepares to use it for the logon session.

During the logon session, the RADIUS server encrypts and sends the WEP key, called a *session key*, over the wired LAN to the access point. The access point encrypts its broadcast key with the session key and sends the encrypted broadcast key to the client, which uses the session key to decrypt it. The client and access point activate WEP and use the session and broadcast WEP keys for all communications during the remainder of the session.

There is more than one type of EAP authentication, but the access point behaves the same way for each type: it relays authentication messages from the wireless client device to the RADIUS server and from the RADIUS server to the wireless client device. See the "Setting Up EAP Authentication" section on page 4-20 for instructions on setting up EAP on the access point.

> ✎
>
> **Note**   If you use EAP authentication, you can select open or shared key authentication, but you don't have to. EAP authentication controls authentication both to your access point and to your network.

• MAC address—The access point relays the wireless client device's MAC address to a RADIUS server on your network, and the server checks the address against a list of allowed MAC addresses. If you don't have a RADIUS server on your network, you can create the list of allowed MAC addresses on the access point's Address Filters page. Devices with MAC addresses not on the list are not allowed to authenticate. Intruders can create counterfeit MAC addresses, so MAC-based authentication is less secure than EAP authentication. However, MAC-based authentication provides an alternate authentication method for client devices that do not have EAP capability. See the "Setting Up MAC-Based Authentication" section on page 4-29 for instructions on enabling MAC-based authentication.

Figure 4-3 shows the authentication sequence for MAC-based authentication.

Figure 4-3   Sequence for MAC-Based Authentication
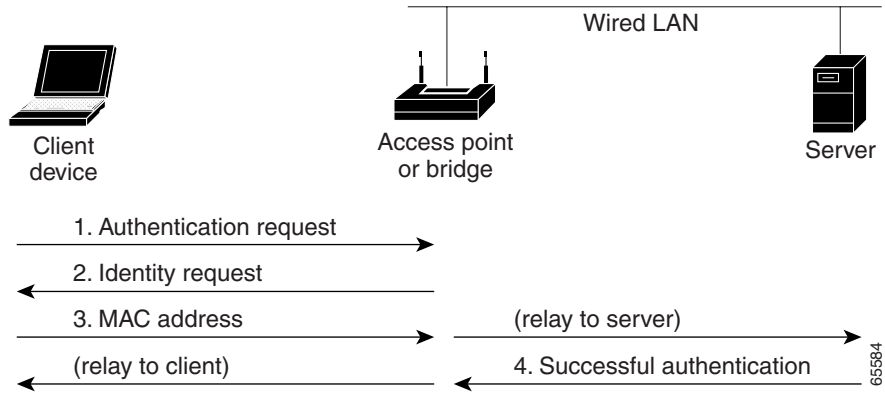
• Open—Allows any device to authenticate and then attempt to communicate with the access point. Using open authentication, any wireless device can authenticate with the access point, but the device can only communicate if its WEP keys match the access point's. Devices not using WEP do not attempt to authenticate with an access point that is using WEP. Open authentication does not rely on a RADIUS server on your network.

Figure 4-4 shows the authentication sequence between a device trying to authenticate and an access point using open authentication. In this example, the device's WEP key does not match the access point's key, so it can authenticate but not pass data.

Figure 4-4   Sequence for Open Authentication
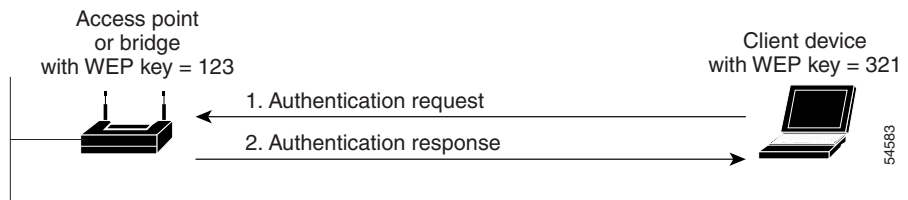
• Shared key—Cisco provides shared key authentication to comply with the IEEE 802.11b standard. However, because of shared key's security flaws, we recommend that you avoid using it.

During shared key authentication, the access point sends an unencrypted challenge text string to any device attempting to communicate with the access point. The device requesting authentication encrypts the challenge text and sends it back to the access point. If the challenge text is encrypted correctly, the access point allows the requesting device to authenticate. Both the unencrypted challenge and the encrypted challenge can be monitored, however, which leaves the access point open to attack from an intruder who calculates the WEP key by comparing the unencrypted and encrypted text strings. Because of this weakness, shared key authentication can be less secure than open authentication. Like open authentication, shared key authentication does not rely on a RADIUS server on your network.

Figure 4-5 shows the authentication sequence between a device trying to authenticate and an access point using shared key authentication. In this example the device's WEP key matches the access point's key, so it can authenticate and communicate.

Figure 4-5   Sequence for Shared Key Authentication
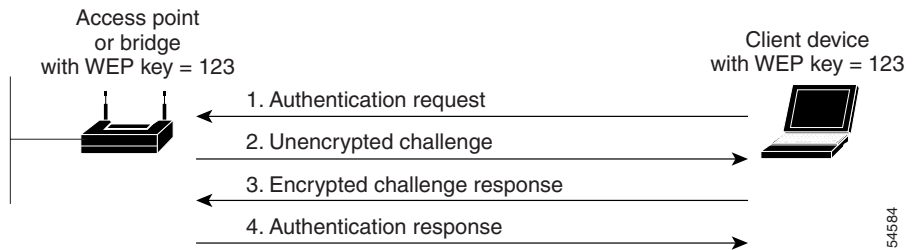
Combining MAC-Based, EAP, and Open Authentication

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 MAC authentication fails, the access point waits for the client device to attempt EAP authentication. See the "Authenticating Client Devices Using MAC Addresses or EAP" section on page 4-34 for more information on this feature.

Protecting the Access Point Configuration with User Manager

The access point's user manager feature prevents unauthorized entry to the access point management system. You create a list of administrators authorized to view and adjust the access point settings; unauthorized users are locked out. See the "Setting Up Administrator Authorization" section on page 4-41 for instructions on using the user manager.

Setting Up WEP

Use the AP Radio Data Encryption pages to set up WEP. You also use the AP Radio Data Encryption pages to select authentication types for the access point. The internal radio and the radio module both have an AP Radio Data Encryption page. Both pages contain the same settings. Figure 4-6 shows the AP Radio Data Encryption page.

Figure 4-6   AP Radio Data Encryption Page

Follow this link path to reach the AP Radio Data Encryption page:

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

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

3. On the Security Setup page, click **Radio Data Encryption (WEP)** for the internal radio or the radio module.

Follow these steps to set up WEP keys and enable WEP:

Step 1 Follow the link path to the AP Radio Data Encryption page.

Step 2 Before you can enable WEP, you must enter a WEP key in at least one of the Encryption Key fields.

> **Note**   If you enable broadcast key rotation and EAP authentication to provide
> client devices with dynamic WEP keys, you can enable WEP without
> entering the keys.

For 40-bit encryption, enter 10 hexadecimal digits; for 128-bit encryption, enter
26 hexadecimal digits. Hexadecimal digits include the numbers 0 through 9 and
the letters A through F. Your 40-bit WEP keys can contain any combination of 10
of these characters; your 128-bit WEP keys can contain any combination of 26 of
these characters. The letters are not case-sensitive.

You can enter up to four WEP keys. The characters you type for a key's contents
appear only when you type them. After you click **Apply** or **OK**, you cannot view
the key's contents.

> **Note**   If you enable EAP authentication, you must select key 1 as the 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. If you
> enable broadcast key rotation, however, you can select key 1 or key 2 as
> the transmit key or you can enable WEP without entering any keys.

Step 3   Use the Key Size pull-down menu to select **40-bit** or **128-bit** encryption for each
key. The **not set** option clears the key. You can disable WEP altogether by
selecting **not set** for each key or by selecting **No Encryption** in Step 5.

Step 4   Select one of the keys as the transmit key. If you select Network-EAP as the
authentication type, select key 1 as the transmit key.

> **Note**   Client devices that do not use EAP to authenticate to the access point must
> contain the access point's transmit key in the same key slot in the client
> devices' WEP key lists. However, the key does not have to be selected as
> the transmit key in the client devices' WEP key lists.

Table 4-1 shows an example WEP key setup that would work for the access point
and an associated device:

Table 4-1   WEP Key Setup Example

Key Slot	Access Point			Associated Device	
	Transmit?	Key Contents	Transmit?	Key Contents
1	x	`12345678901234567890abcdef`	—	`12345678901234567890abcdef`
2	—	`09876543210987654321fedcba`	x	`09876543210987654321fedcba`
3	—	not set	—	not set
4	—	not set	—	`FEDCBA09876543211234567890`

Because the access point's WEP key 1 is selected as the transmit key, WEP key 1 on the other device must contain the same contents. WEP key 4 on the other device is set, but because it is not selected as the transmit key, WEP key 4 on the access point does not need to be set at all.

✎

Note If you enable MIC but you use static WEP (you do not enable any type of EAP authentication), both the access point and any devices with which it communicates must use the same WEP key for transmitting data. For example, if the MIC-enabled access point uses the key in slot 1 as the transmit key, a client device associated to the access point must use the same key in its slot 1, and the key in the client's slot 1 must be selected as the transmit key.

The characters you type for the key contents appear only when you type them. After you click **Apply** or **OK**, you cannot view the key contents. Select **Not set** from the Key Size pull-down menu to clear a key.

Step 5 Select **Optional** or **Full Encryption** from the pull-down menu labeled *Use of Data Encryption by Stations is*.

✎

Note You must set a WEP key before enabling WEP. The options in the *Use of Data Encryption by Stations is* pull-down menu do not appear until you set a key.

The three settings in the pull-down menu include:

- No Encryption (default)—The access point communicates only with client devices that are not using WEP. Use this option to disable WEP.

- Optional—Client devices can communicate with the access point either with or without WEP.

> ✎
>
> **Note**   If you select Optional, Cisco Aironet client devices associating to the access point must be configured to allow association to mixed cells. See the *Cisco Aironet Wireless LAN Adapters Software Configuration Guide* for instructions on configuring Cisco Aironet client devices.

- Full Encryption—Client devices must use WEP when communicating with the access point. Devices not using WEP are not allowed to communicate.

> ✎
>
> **Note**   You must select Full Encryption to enable Message Integrity Check (MIC). See the "Enabling Message Integrity Check (MIC)" section on page 4-14 for instructions on setting up MIC.

Step 6   Click **OK**. You return automatically to the Security Setup page.

Using SNMP to Set Up WEP

You can use SNMP to set the WEP level on the access point. Consult the "Using SNMP" section on page 2-10 for details on using SNMP.

Access points use the following SNMP variables to set the WEP level:

- dot11ExcludeUnencrypted.2
- awcDot11AllowEncrypted.2

Table 4-2 lists the SNMP variable settings and the corresponding WEP levels.

Table 4-2   SNMP Variable Settings and Corresponding WEP Levels

SNMP Variable	WEP Full	WEP Off	WEP Optional
dot11ExcludeUnencrypted.2	true	false	false
awcDot11AllowEncrypted.2	true	false	true

> **Note**   Access points do not use the SNMP variable *dot11PrivacyInvoked*, so it is always set to disabled.

Enabling Additional WEP Security Features

You can enable three advanced security features to protect against sophisticated attacks on your wireless network's WEP keys. This section describes how to set up and enable these features:

- Enabling Message Integrity Check (MIC)
- Enabling Temporal Key Integrity Protocol (TKIP)
- Enabling Broadcast WEP Key Rotation

Enabling Message Integrity Check (MIC)

MIC prevents attacks on encrypted packets called *bit-flip* attacks. During a bit-flip attack, an intruder intercepts an encrypted message, alters it slightly, and retransmits it, and the receiver accepts the retransmitted message as legitimate. The MIC, implemented on both the access point and all associated client devices, adds a few bytes to each packet to make the packets tamper-proof.

> **Note**   You must set up and enable WEP with full encryption before MIC takes effect.

![Note icon]

Note   To use MIC, the Use Aironet Extensions setting on the radio's AP Radio
         Advanced page must be set to yes (the default setting).

![Note icon]

Note   Enabling MIC on the internal radio module might reduce throughput for that radio
         by as much as 30%.

Use the AP Radio Advanced page to enable MIC. Both the internal radio and the
radio module have an AP Radio Advanced page. Both pages contain the same
settings. Figure 4-7 shows the AP Radio Advanced page for the internal radio.

Figure 4-7   AP Radio Advanced Page for Internal Radio

Follow this link path to browse to the AP Radio Advanced page:

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

2. On the Setup page, click **Advanced** in the AP Radio row under Network Ports for the internal radio or the radio module.

Follow these steps to enable MIC:

Step 1   Follow the steps in the "Setting Up WEP" section on page 4-9 to set up and enable WEP. You must set up and enable WEP with full encryption before MIC becomes active. If WEP is off or if you set it to optional, MIC is not enabled.

> ✎
>
> **Note**   If you enable MIC but you use static WEP (you do not enable any type of EAP authentication), both the access point radio and any devices with which it communicates must use the same WEP key for transmitting data. For example, if the MIC-enabled access point uses the key in slot 1 as the transmit key, a client device associated to the access point must use the same key in its slot 1, and the key in the client's slot 1 must be selected as the transmit key.

Step 2   Browse to the AP Radio Advanced page for the internal radio or the radio module.

Step 3   Select **MMH** from the Enhanced MIC verification for WEP pull-down menu.

Step 4   Make sure **yes** is selected for the Use Aironet Extensions setting. MIC does not work if Use Aironet Extensions is set to no.

Step 5   Click **OK**. MIC is enabled, and only client devices with MIC capability can communicate with the access point.

Enabling Temporal Key Integrity Protocol (TKIP)

Temporal Key Integrity Protocol (TKIP), also known as WEP key hashing, defends against an attack on WEP in which the intruder uses an unencrypted segment called the initialization vector (IV) in encrypted packets to calculate the WEP key. TKIP removes the predictability that an intruder relies on to determine the WEP key by exploiting IVs. TKIP protects both unicast and broadcast WEP keys.

Note   When you enable TKIP, all WEP-enabled client devices associated to the access point must support WEP key hashing. WEP-enabled devices that do not support key hashing cannot communicate with the access point.

Note   To use TKIP, the Use Aironet Extensions setting on the AP Radio Advanced page must be set to **yes** (the default setting).

Tip   When you enable TKIP, you do not need to enable broadcast key rotation. Key hashing prevents intruders from calculating the static broadcast key, so you do not need to rotate the broadcast key.

Follow these steps to enable TKIP:

Step 1   Follow the steps in the "Setting Up WEP" section on page 4-9 to set up and enable WEP. Select either optional or full encryption for the WEP level.

Step 2   Follow this link path to browse to the AP Radio Advanced page:

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

   b.   On the Setup page, click **Advanced** in the AP Radio row under Network Ports for the internal radio or the radio module.

Step 3   Select **Cisco** from the Temporal Key Integrity Protocol pull-down menu.

Step 4   Make sure **yes** is selected for the Use Aironet Extensions setting. Key hashing does not work if Use Aironet Extensions is set to no.

Step 5   Click **OK**. TKIP is enabled.

Enabling Broadcast WEP Key Rotation

EAP authentication provides dynamic unicast WEP keys for client devices but uses static multicast keys. With broadcast, or multicast, WEP key rotation enabled, the access point provides a dynamic broadcast WEP key and changes it at the interval you select. Broadcast key rotation is an excellent alternative to TKIP if your wireless LAN supports wireless client devices that are not Cisco devices or that cannot be upgraded to the latest firmware for Cisco client devices.

Note When you enable broadcast key rotation, only wireless client devices using LEAP or EAP-TLS authentication can use the access point. Client devices using static WEP (with open, shared key, or EAP-MD5 authentication) cannot use the access point when you enable broadcast key rotation.

Note If you enable Broadcast Key Rotation on one of the radios in a dual-radio access point, Broadcast Key Rotation is automatically enabled on the other radio.

Tip You might not need to enable broadcast key rotation if you enable TKIP. You can use both key rotation and key hashing, but these features provide similar protection.

Follow these steps to enable broadcast key rotation:

Step 1 Follow the steps in the "Setting Up WEP" section on page 4-9 to set up and enable WEP.

Step 2 Follow this link path to browse to the AP Radio Advanced page:

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

   b. On the Setup page, click **Advanced** in the AP Radio row under Network Ports for the internal radio or the radio module.

Step 3 On the AP Radio Advanced page, enter the rotation interval in seconds in the Broadcast WEP Key rotation interval entry field. If you enter 900, for example, the access point sends a new broadcast WEP key to all associated client devices every 15 minutes. To disable broadcast WEP key rotation, enter **0**.

Note You must set the rotation interval on every access point using broadcast key rotation. You cannot enter the rotation interval on your RADIUS server.

Tip Use a short rotation interval if the traffic on your wireless network contains numerous broadcast or multicast packets.

Step 4 Click **OK**. Broadcast key rotation is enabled.

Setting Up Open or Shared Key Authentication

Cisco recommends Open authentication as preferable to Shared Key authentication. The challenge queries and responses used in Shared Key leave the access point particularly vulnerable to intruders.

Use the AP Radio Data Encryption page to select Open or Shared Key authentication. The internal radio and the radio module both have an AP Radio Data Encryption page. Both pages contain the same settings. Figure 4-6 shows the AP Radio Data Encryption page for the internal radio.

Follow these steps to select Open or Shared Key authentication:

Step 1 Follow the instructions in the "Setting Up WEP" section on page 4-9 to set up and enable WEP.

You must enable WEP to use shared key authentication, but you do not have to enable WEP to use open authentication. However, Cisco strongly recommends that you enable WEP on all wireless networks.

Step 2 Select **Open** (default) or **Shared Key** to set the authentications the access point recognizes. You can select all three authentication types.

Step 3 If you want to force all client devices to perform EAP authentication before joining the network, select the **Require EAP** checkbox under Open or Shared. Selecting the Require EAP checkbox also allows client devices using various types of EAP authentication, including EAP-TLS and EAP-MD5, to authenticate through the access point. To allow LEAP-enabled client devices to authenticate

through the access point, you should also select **Network-EAP**. See the "Setting Up EAP Authentication" section on page 4-20 for details on the Require EAP and Network-EAP settings.

Step 4   Click **OK**. You return automatically to the Security Setup page.

Setting Up EAP Authentication

During EAP authentication, the access point relays authentication messages between the RADIUS server on your network and the authenticating client device. This section provides instructions for:

- Enabling EAP on the Access Point
- Enabling EAP in Cisco Secure ACS
- Setting up a Repeater Access Point as a LEAP Client

Enabling EAP on the Access Point

You use the Authenticator Configuration page and the AP Radio Data Encryption pages to set up and enable EAP authentication. The internal radio and the radio module both have an AP Radio Data Encryption page. Both pages contain the same settings. Figure 4-6 shows the AP Radio Data Encryption page for the internal radio. Figure 4-8 shows the Authenticator Configuration page.

Figure 4-8   Authenticator Configuration Page

Follow this link path to reach the Authenticator Configuration page:

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

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

3. On the Security Setup page, click **Authentication Server**.

Follow these steps to enable EAP on the access point:

Step 1   Follow the link path to the Authenticator Configuration page.

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.

✎

Note   You can use the same server for both EAP authentication and MAC-address authentication.

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 will use. EAP operates only when the radio firmware on client devices complies with the same 802.1X Protocol draft as the management firmware on the access point. If the radio firmware on the client devices that will associate with the access point is 4.16, for example, you should select **Draft 8**. Menu options include:

- Draft 7—No radio firmware versions compliant with Draft 7 have LEAP capability, so do not 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—Select this option if client devices that associate with this access point use Microsoft Windows XP authentication or if LEAP-enabled client devices that associate with this access point use radio firmware version 4.25 or later.

Note   Functionality in Draft 10 is equivalent to the functionality in Draft 11, the ratified draft of the 802.1X standard.

Table 4-3 lists radio firmware versions for Cisco Aironet products and the drafts with which they comply.

Table 4-3   802.1x Protocol Drafts and Compliant Client Firmware

Firmware Version	Draft 7	Draft 8	Draft 10[1]
PC/PCI cards 4.13	—	x	—
PC/PCI cards 4.16	—	x	—
PC/PCI cards 4.23	—	x	—
PC/PCI cards 4.25 and later	—	—	x
WGB34x/352 8.58	—	x	—
WGB34x/352 8.61 or later	—	—	x
AP34x/35x 11.05 and earlier	—	x	—
AP34x/35x 11.06 and later[2]	—	x	x
BR352 11.06 and later[1]	—	x	x

1. Functionality in Draft 10 is equivalent to the functionality in Draft 11, the ratified draft of the 802.1X standard.

2. 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.

Step 3   Enter the name or IP address of the RADIUS server in the Server Name/IP entry field.

Step 4   Enter the port number your RADIUS 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 5   Enter the shared secret used by your RADIUS server in the Shared Secret entry field. The shared secret on the access point must match the shared secret on the RADIUS server. The shared secret can contain up to 64 alphanumeric characters.

Step 6   Enter the number of seconds the access point should wait before authentication fails. If the server does not respond within this time, the access point tries to contact the next authentication server in the list if one is specified. Other backup servers are used in list order when the previous server times out.

Step 7   Select **EAP Authentication** under the server. The EAP Authentication checkbox designates the server as an authenticator for any EAP type, including LEAP, EAP-TLS, and EAP-MD5.

Step 8   Click **OK**. You return automatically to the Security Setup page.

Step 9   On the Security Setup page, click **Radio Data Encryption (WEP)** for the internal radio or the radio module to browse to the radio's AP Radio Data Encryption page.

Step 10   Select **Network-EAP** for the Authentication Type setting to allow EAP-enabled client devices to authenticate through the access point.

Select **Require EAP** under Open or Shared Key to allow client devices with EAP-TLS or EAP-MD5 enabled through Windows XP to authenticate through the access point. If you do not select Require EAP, client devices with EAP enabled through Windows XP authenticate to the access point but might not perform

mutual EAP authentication with your RADIUS server. LEAP-enabled client devices perform LEAP authentication through the access point even if you do not select Require EAP.

✎
Note   When you select Require EAP, you block client devices that are not using EAP from authenticating through this access point radio.

Table 4-4 lists the access point settings that provide authentication for various client devices.

Table 4-4   Access Point EAP Settings for Various Client Configurations

Access Point Configuration	Client Devices Allowed to Authenticate
Network-EAP authentication	• Client devices with LEAP enabled • Repeater access points with LEAP enabled
Open authentication with Require EAP checkbox selected	• Client devices with EAP enabled • Cisco Aironet devices with EAP-TLS or EAP-MD5 enabled through Windows XP **Note** Selecting Require EAP on the access point blocks non-EAP client devices from using the access point.

Step 11   Check that a WEP key has been entered in key slot 1. If a WEP key has been set up in slot 1, skip to Step 15. If no WEP key has been set up, proceed to Step 12.

✎
Note   You can use EAP without enabling WEP, but packets sent between the access point and the client device will not be encrypted. To maintain secure communications, use WEP at all times.

Step 12   Enter a WEP key in slot 1 of the Encryption Key fields. The access point uses this key for multicast data signals (signals sent from the access point to several client devices at once). This key does not need to be set on client devices.

Step 13   Select **128-bit** encryption from the Key Size pull-down menu.

Step 14   If the key in slot 1 is the only WEP key set up, select it as the transmit key.

Step 15   Click **OK**. You return automatically to the Security Setup page.

Enabling EAP in Cisco Secure ACS

Cisco Secure Access Control Server for Windows NT/2000 Servers (Cisco Secure ACS) is network security software that helps authenticate users by controlling access to a network access server (NAS) device, such as an access server, PIX Firewall, router, or wireless access point or bridge.

Cisco Secure ACS operates as a Windows NT or Windows 2000 service and controls the authentication, authorization, and accounting (AAA) of users accessing networks. Cisco Secure ACS operates with Windows NT 4.0 Server and Windows 2000 Server.

> **Note**   You must use ACS version 2.6 or later to set up the access point in ACS.

Follow these steps to include the access point as a Network Access Server (NAS) in Cisco Secure ACS:

Step 1   On the ACS main menu, click **Network Configuration**.

Step 2   Click **Add New Access Server**.

Step 3   In the **Network Access Server Hostname** entry field, type the name you want to assign to the access point as an access server.

> **Note**   This field does not appear if you are configuring an existing NAS.

Step 4   In the **Network Access Server IP address** box, type the access point's IP address.

Step 5   In the **Key** box, type the shared secret that the TACACS+ or RADIUS NAS and Cisco Secure ACS use to encrypt the data. For correct operation, the identical key (case sensitive) must be configured on the access point's Authenticator Configuration page and in Cisco Secure ACS.

Step 6   From the **Authenticate Using** drop-down menu, select **RADIUS (Cisco Aironet)**.

Step 7 To save your changes and apply them immediately, click the **Submit + Restart** button.

Tip To save your changes and apply them later, click **Submit**. When you are ready to implement the changes, select **System Configuration > Service Control** and click **Restart**.

Note Restarting the service clears the Logged-in User Report, refreshes the Max Sessions counter, and temporarily interrupts all Cisco Secure ACS services.

Setting a Session-Based WEP Key Timeout

You can set a timeout value for the session-based WEP key. When the timeout value elapses, the server issues a new dynamic WEP key for authenticated client devices.

Note If you enable TKIP on the access point, you do not need to set up a session-based WEP key timeout. You can use both TKIP and a session key timeout, but these features provide redundant protection.

You should consider several factors when determining the best session key timeout value for your wireless network. Consult *Product Bulletin 1515: Cisco Wireless LAN Security Bulletin* for guidelines on selecting timeout values. Use this URL to browse to Product Bulletin 1515:

http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1515_pp.htm

Follow these steps to set a timeout value for session-based WEP keys:

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

Step 2 In the Group drop-down menu, select the group for which you want to modify the WEP key/session timeout. The **Default** group is usually the group you need to modify.

Step 3   Click **Edit Settings**.

Step 4   Scroll down to the IETF RADIUS Attributes settings.

Step 5   Select the checkbox for [027] Session-Timeout and enter the number of seconds for your timeout value in the [027] Session-Timeout entry field.

Step 6   Click **Submit + Restart**. The timeout value is enabled.

Setting up a Repeater Access Point as a LEAP Client

If you configure one or both of your access point radios as a repeater (an access point not connected to the wired LAN), you can set up the repeater radio to authenticate to your network like other wireless client devices. After you provide a network username and password for the repeater radio, it authenticates to your network using LEAP, Cisco's wireless authentication method, and receives and uses dynamic WEP keys.

See the "Setting Up a Repeater Access Point" section on page 8-1 for instructions on setting up a repeater access point.

Follow these steps to enable LEAP authentication on a repeater radio:

Step 1   Set up a username and password on your network just as you would for a new user. The repeater radio will use this username and password to authenticate.

Step 2   Follow this link path to browse to the radio's 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 for the internal radio or the radio module.

Figure 4-9 shows the AP Radio Identification page for the internal radio.

Figure 4-9   AP Radio Identification Page for Internal Radio

Step 3   Enter the network username you set up for the radio in Step 1 in the LEAP User Name entry field.

Step 4   Enter the network password you set up for the radio in Step 1 in the LEAP Password entry field.

Step 5   Click **OK**.

Step 6   Follow the steps in the "Enabling EAP on the Access Point" section on page 4-20 to enable Network-EAP on the repeater access point.

The next time the repeater reboots, it performs LEAP authentication and associates to the root access point.

✎

Note   If the repeater access point fails to authenticate because the root access point or the RADIUS server is not set up correctly, you must reboot the repeater access point after correcting the problem. The repeater access point does not attempt to reauthenticate until it reboots.

Setting Up MAC-Based Authentication

MAC-based authentication allows only client devices with specified MAC addresses to associate and pass data through the access point. Client devices with MAC addresses not in a list of allowed MAC addresses are not allowed to associate with the access point. You can create a list of allowed MAC addresses in the access point management system or on a server used for MAC-based authentication, and you can enable MAC-based authentication on one or both of the access point radios.

This section provides instructions for:

- Enabling MAC-Based Authentication on the Access Point
- Authenticating Client Devices Using MAC Addresses or EAP
- Enabling MAC-Based Authentication in Cisco Secure ACS

Enabling MAC-Based Authentication on the Access Point

Follow these steps to set up and enable MAC-based authentication on the access point:

Step 1   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.

Figure 4-10 shows the Address Filters page.

Figure 4-10   Address Filters Page

Note Step 2 and Step 3 describe entering MAC addresses in the access point management system. If you will enter MAC addresses only in a list used by the authentication server, skip to Step 4.

Step 2 Type a MAC address in the Dest MAC Address field. You can type the address with colons separating the character pairs (00:40:96:12:34:56, for example) or without any intervening characters (004096123456, for example).

Make sure the **Allowed** option is selected under the Dest MAC Address field.

Step 3 Click **Add**. The MAC address appears in the Existing MAC Address Filters list. The MAC address remains in the management system until you remove it. To remove the MAC address from the list, select it and click **Remove**.

Note Be sure to enter your own MAC address in the list of allowed addresses.

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

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 access point 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 to avoid losing your connection to the access point.

Step 14 You can enable MAC authentication on one or both of the access point radios on the AP Radio Advanced pages. Click **Advanced** for the internal radio or the radio module in the AP Radio row of the Network Ports section at the bottom of the Setup page. The radio's AP Radio Advanced page appears. Figure 4-12 shows the AP Radio Advanced page for the internal radio.

Figure 4-12 AP Radio Advanced Page

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 radio 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 radio 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 radio are not immediately affected when you set the 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 through this radio 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 one or both access point radios 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 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 IEEE 802.11 open authentication:

Step 1   Follow the steps in the "Setting Up EAP Authentication" section on page 4-20 to set up EAP. You must select **Require EAP** under Open authentication on the radio's 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 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 your connection 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 for the internal radio or the radio module (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 for the internal radio or the radio module (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 for the internal radio or the radio module (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 for the internal radio or the radio module (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 4-20 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

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 icon]

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

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

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

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.

C H A P T E R   **5**

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

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 3-64.

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

Home	Map	Network	Associations	Setup	Logs	Help	2000/11/15 11:26:16

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

Number of Pkts. [5]   Pkt. Size [64]   [Refresh] [Ping]

Number of Pkts. [100]   Pkt. Size [500]   [Link Test]

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	108	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.	80%

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 3-22 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 "Settings on the Association Table Advanced Page" section on page 3-69 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. The ping button might not appear if the access point cannot detect the device's IP address.

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
```

Test Again

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

Test Again   Continuous Test

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
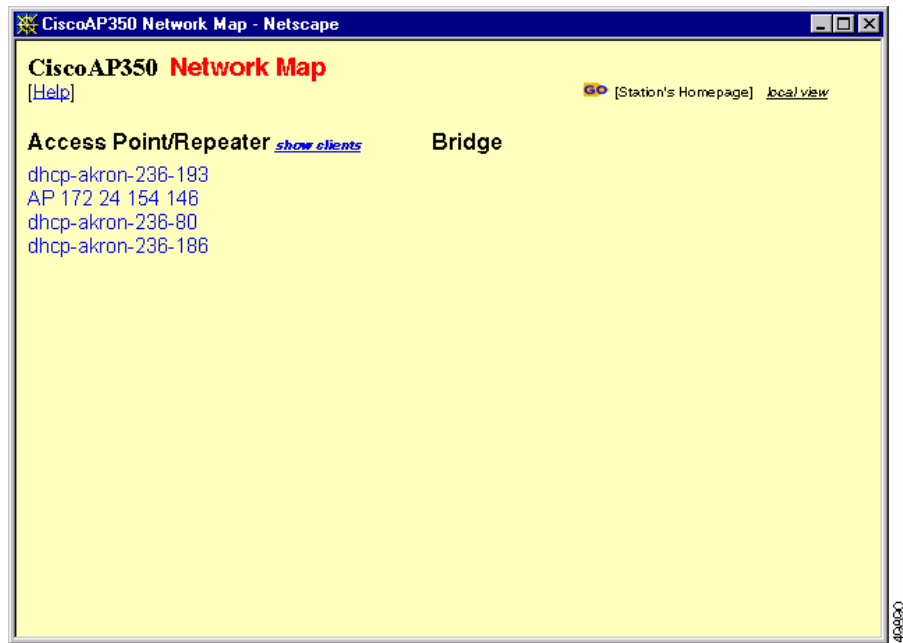
Click the name of a wireless device to open a new browser window displaying a Station page displaying the access point's local information for that device. Click **Go** beside the device name to open a new browser window displaying that device's home page, if available. Some devices, such as PC card 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

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 Internal or AP Radio Module—This checkbox appears when one of the access point radios 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

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

The Port Assignments page contains these settings for the internal radio ports and the radio module ports:

- 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

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

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.

Enabling Wireless Network Accounting

6

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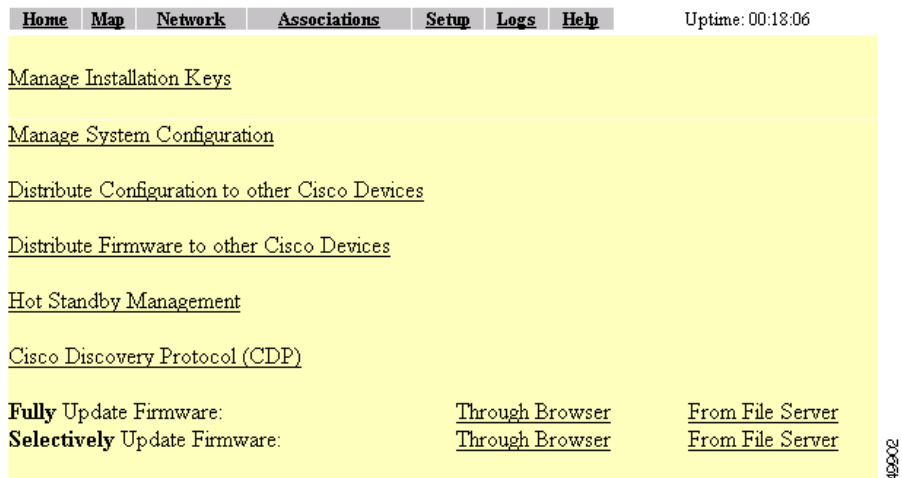
Follow this link path in the browser interface to reach the Cisco Services Setup page:

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 four firmware components—the management system firmware, the firmware web pages, and the radio firmware for both radios—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

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.

✎
Note   The access point only updates the radio firmware if the radio firmware version to be loaded is newer than the firmware in the radio.

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

Follow these steps to update one of the 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 four firmware components—the management system firmware, the firmware web pages, and the radio firmware for both radios—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

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

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.

✎

Note   The access point only updates the radio firmware if the radio firmware version to be loaded is newer than the firmware in the radio.

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

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

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 11.40 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 3-55)
- 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)

Follow the steps in the "Limiting Distributions" section on page 6-11 to limit the firmware distribution to certain access points.

Figure 6-7   Distribute Firmware Page

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

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 11.40 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 3-55)

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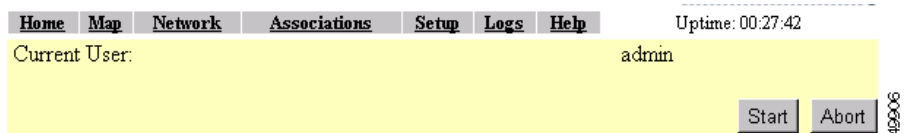
Follow this link path in the browser interface to reach the Distribute Configuration page:

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**.

Limiting Distributions

You might need to distribute a configuration or firmware to certain access points but not to others. For example, if you distribute a configuration to several access points that use non-overlapping channels, the distributed configuration overwrites the channel settings and puts all the access points on the same channel. In this example, after the distribution you have to reconfigure all the access points to set up non-overlapping channels.

The simplest way to limit the distribution of a configuration or firmware is to create a unique user in the distributing and receiving access points' user management systems. An access point accepts distributed firmware and configurations only if its user manager contains 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).

Follow these steps to limit distributions:

Step 1   On the distributing access point, browse to the Security Setup page and create a new user, and then enable user manager protection. See the "Creating a List of Authorized Management System Users" section on page 4-42 section for complete instructions on creating a new user.

Step 2   Create the same user with the same password and capabilities on each access point that should receive the distributed firmware or configuration. Make sure user manager protection is enabled on the access points.

Step 3   Log into the distributing access point using the new user name and perform the distribution. Only access points with matching users in their user manager systems receive the distribution.

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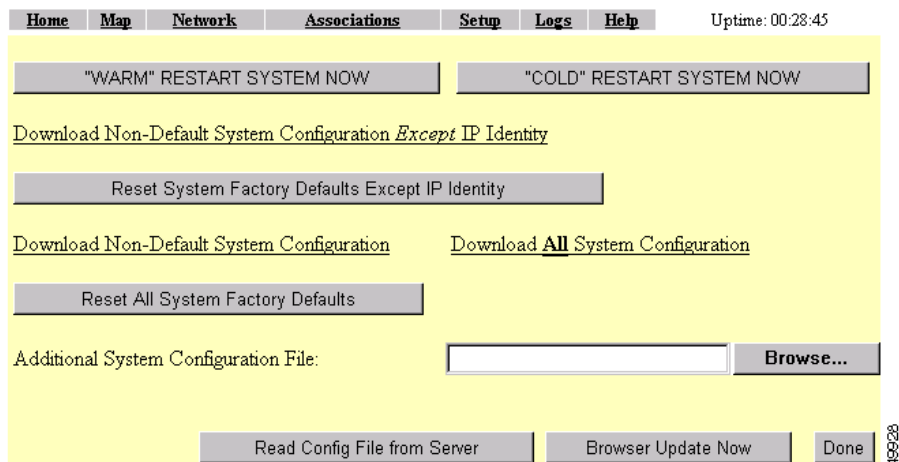
Follow this link path in the browser interface to reach the System Configuration Setup page:

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

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 9-43.

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.

■ **Downloading, Uploading, and Resetting the Configuration**

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

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 2-10.

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

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 None.

- 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.

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

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.

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

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.

You can set up either of the radios in your access point as a repeater; one radio must be set up as a root unit. When one of the radios is a repeater, the access point's Ethernet port is blocked. However, you can still configure the access point through the Ethernet port using a crossover cable when the repeater link is disactivated. Figure 8-1 shows an access point acting as a repeater.

Figure 8-1   Access Point as Repeater
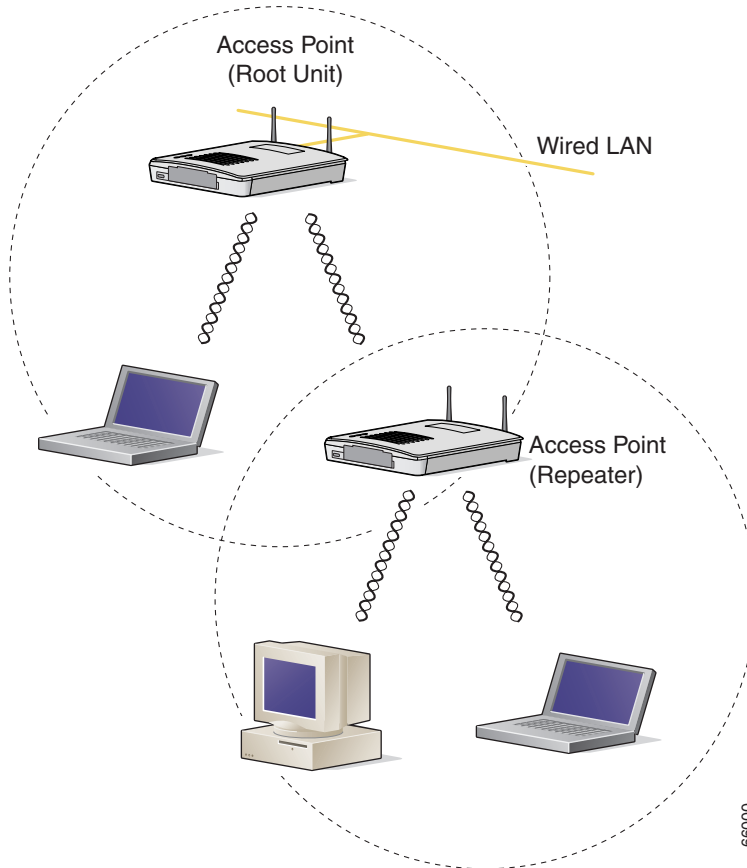
You can set up a chain of several repeater access points, but throughput for client devices at the end of the repeater chain will be quite low. Because each repeater must receive and then re-transmit each packet on the same channel, throughput is cut in half for each repeater you add to the chain.

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 1200 Series 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 for the root radio (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 Connect power to the repeater access point. Consult the the *Quick Start Guide: Cisco 1200 Series Aironet Access Points* for power options.

> ✎
>
> **Note** If both radios are set up as repeaters, the access point will not be connected to the wired LAN. Therefore, if you use a power injector, do not run Ethernet cable from the power injector to a switch.

Step 6 Connect a DB-9 to RJ-45 serial cable to the COM port on a computer and to the RJ-45 serial port on the access point.

Step 7 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 No flow control.

Step 8 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 9 On the Express Setup page, enter the same SSID that is set on the root access point.

> ✎
>
> **Note** Step 10 and Step 11 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 12.

Step 10 On the Express Setup page, enter a fixed IP address for the repeater access point in the Default IP address field.

Step 11 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 12 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 16.

**Step 13** On the AP Radio Hardware page, enter the same settings for Data Rates that are on the root access point.

Step 14   On the AP Radio Data Encryption page, enter the same WEP key settings that are on the root access point.

Step 15   Also on the AP Radio Data Encryption page, select the same Authentication Types that are on the root access point.

Step 16   On the AP Radio Advanced page, enter the root access point's MAC address in the Specified access point 1 entry field.

Step 17   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 18   The status LED on the root access point should be steady green, indicating that at least one client device is associated to it. The status LED on the repeater access point is steady green when it is associated to the root access point and has client devices associated to 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 to the root access point but has no client devices associated to it. The repeater access point should also appear as associated to 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 to 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

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.

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.

> ✎
>
> **Note**   The access point performs the carrier test for the internal radio only; it does not perform the carrier test for the radio module.

Figure 9-1 shows the Radio Diagnostics page.

Figure 9-1   Radio Diagnostics Page

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%

82147

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's internal radio. The access point does not perform the carrier test for the radio module.

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
```

Stop Test
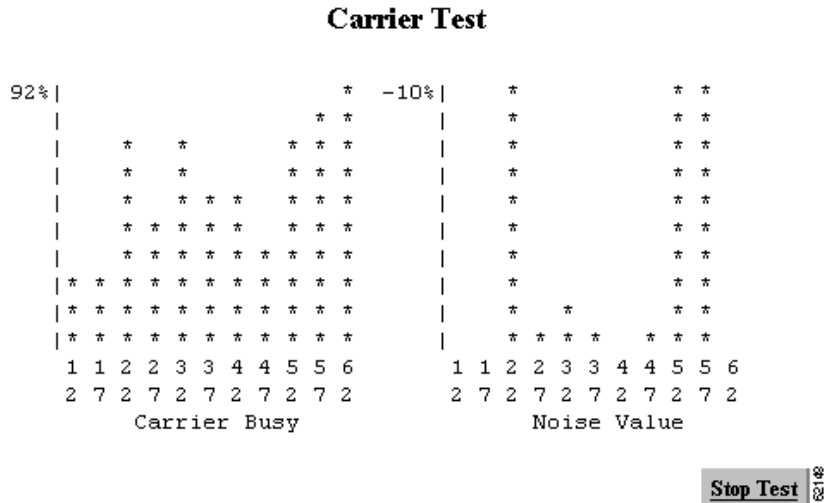
The bar graph on the left side of the window displays the percentage used for each frequency; the highest current percentage used is labeled on the top left of the graph. In this example, the highest percentage used for any frequency is 77. The access point's available frequencies are listed vertically 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. 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

Name	Ethernet*	AP Radio: Internal	AP Radio: Module
Status	Up	Up	Up
Max. Mb/s	100.0	11.0	54.0
IP Addr.	192.168.1.14	192.168.1.14	192.168.1.14
MAC Addr.	00059a384281	00059a384281	00059a384281
Radio SSID		tsk_buckeye_leap2g	tsk_buckeye_leap5g
Receive			
unicast pkts.	73943631	0	77908752
multicast pkts.	335508	0	0
total bytes	1939264140	0	127523138
errors	0	0	12
discards	0	0	1
forwardable pkts.	74271261	0	77905687
filtered pkts.	160598	0	0
Transmit			
unicast pkts.	77915236	0	73927630
multicast pkts.	32129	0	217001
total bytes	2091376161	0	4156985469
errors	2	0	421
discards	0	0	0
forwarded pkts.	155867734	0	148262974

Home | Map | Network | Associations | Setup | Logs | Help   2002/06/03 10:52:21

74748

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 9-9 for information on the Ethernet Port page and the "AP Radio Page" section on page 9-12 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 3-20 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

| Home | Map | Network | Associations | Setup | Logs | Help | | 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: Internal** or **AP Radio: Module** in the Network Ports table, the browser displays the AP Radio Port page for the internal radio or for the radio module. This page lists detailed statistics on the radio. Both radios have an AP Radio page, and both pages contain similar information. Figure 9-6 shows an AP Radio Port page example.

Figure 9-6   AP Radio Port Page

| Home | Map | Network | Associations | Setup | Logs | Help | Uptime: 03:23:50 |

Options: Detailed Config. ☐   Detailed Stats. ☐   Individual Rates ☐   [Apply]

Configuration			Set Properties
Status of "awc0"	Up	Maximum Rate (Mb/s)	11.0
IP Address	161.44.236.134	MAC Address	00409625854d
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 3-22 for details on the AP Radio Hardware page.

- Status of "awc0"—*awc0* (Aironet Wireless Communications) is part of Cisco Aironet's naming convention for this radio. This field displays one of three possible operating states:

  - Up—The port is operating properly.

- – Down—The port is not operating.

- – Error—The port is in an error condition.

- Maximum Rate (Mbps)—Maximum rate of data transmission in megabits per second. Data rates set to basic are followed by B.

- IP Addr.—The IP address of the radio port.

- MAC (Media Access Control) Addr.—A unique identifier assigned to the network interface by the manufacturer.

- SSID—The unique identifier that client devices use to associate with the access point radio. The SSID helps client devices distinguish between multiple wireless networks in the same vicinity.

- Operational Rates—The data transmission rates supported and enabled by the access point for communication with client devices.

- Transmit Power (mW)—The power level of radio transmission. You can reduce the transmit power to conserve power or reduce interference. Click **Set Properties** to display the AP Radio Hardware page, where you can change this setting.

Receive Statistics

- Unicast Packets—The number of packets received in point-to-point communication.

- Multicast Packets—The number of packets received that were sent as a transmission to a set of nodes.

- Total Bytes—The total number of bytes received.

- Total Errors—The total number of packets determined to be in error.

- Discarded Packets—Packets discarded due to errors or network congestion.

- Forwardable Packets—Packets received by the port that were acceptable or passable through the filters.

- Filtered Packets—Packets that were stopped or screened by the filters set up on the port.

- Packet CRC Errors—Cyclic redundancy check (CRC) errors that were detected in a received packet.

- Packet WEP Errors—Encryption errors received through this port.

- Overrun Packets—Packets that were discarded because the access point had a temporary overload of packets to handle.

- Duplicate Packets—Packets that were received twice because an acknowledgment was lost and the sender retransmitted the packet.

- Lifetime Exceeded—Fragmented packets that were dropped because it took too long to get the next fragment.

- MIC Packets—Total number of packets received over this radio since system startup and for which a MIC has been requested to be validated with the MMH algorithm.

- MIC Errors—Total number of packets received over this radio since system startup that failed MIC validation with the MMH algorithm.

- MIC Sequ. Errors—Total number of packets received over this radio since system startup that failed MIC validation with the MMH algorithm specifically due to sequence number and duplicate packet errors.

- MIC Auth. Errors—Total number of packets received over this radio since system startup that failed MIC validation with the MMH algorithm specifically due to cryptographic key-mismatch errors.

Transmit Statistics

- Unicast Packets—The number of packets transmitted in point-to-point communication.

- Multicast Packets—The number of packets transmitted that were sent as a transmission to a set of nodes.

- Total Bytes—The number of bytes transmitted from the port.

- Total Errors—The number of packets determined to be in error.

- Discarded Packets—The number of packets discarded by the access point due to errors or network congestion.

- Forwarded Packets—The number of packets transmitted by the port that were acceptable or passable through the filters.

- Max Retry Packets—The number of times request to send (RTS) reached the maximum retry number. Click **Set Properties** to display the AP Radio Hardware page, where you can set the maximum RTS value.

- Total Retries—The total number of retries that occurred through the radio port.

- Canceled Assoc. Lost—Packets dropped because a client device lost association with the access point.

- Canceled AID—Packets dropped by a repeater because it roamed to a different parent during a retransmission attempt.

- Lifetime Exceeded—Fragmented packets that were dropped because it took too long to deliver a fragment.

- MIC Packets—Total number of packets for which the access point has requested MIC has been requested to be calculated with the MMH algorithm before being submitted for transmission over this radio since system startup.

- MIC Errors—Total number of packets which have failed MIC calculation with the MMH algorithm before being submitted for transmission over this radio since system startup.

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

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

Home	Map	Network	Associations	Setup	Logs	Help	Uptime: 03:27:11

Event Severity Level	**Total Events**
System Fatal	0
Protocol Fatal	0
Network Port Fatal	0
System Alert	0
Protocol Alert	0
Network Port Alert	0
External Alert	0
System Warning	0
Protocol Warning	2
Network Port Warning	0
External Warning	0
System Information	0
Protocol Information	21
Network Port Information	21
External Information	1

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

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 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.

Table 9-2   Flag Definitions

Flag Value	Definition
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 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 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 3-9.

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 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 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 top of the access point. Table 9-3 lists the meanings of the indicator signals.

Figure 9-9   Top Panel Indicator Lights
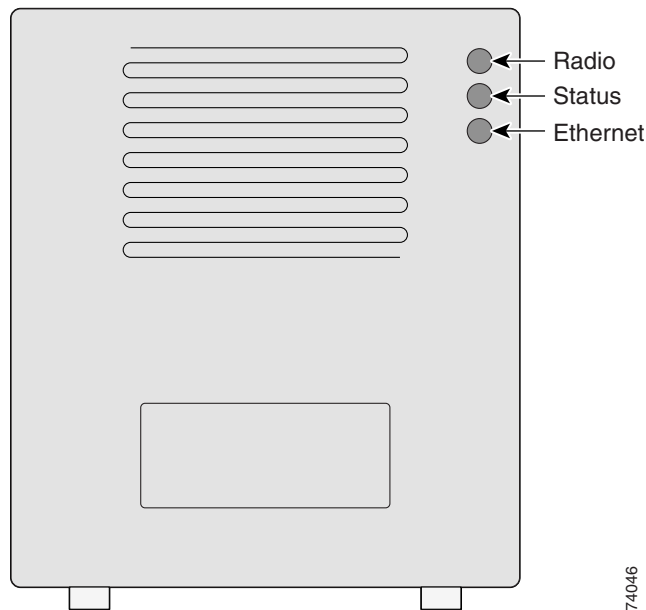
- The Ethernet indicator signals traffic on the wired LAN, or Ethernet infrastructure. This indicator blinks green when a packet is received or transmitted over the Ethernet infrastructure.

- 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 one of the access point radios.

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 to 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 one of the radios.
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[1]
PC/PCI cards 4.13	—	x	—
PC/PCI cards 4.16	—	x	—

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

Firmware Version	Draft 7	Draft 8	Draft 10[1]
PC/PCI cards 4.23	—	x	—
PC/PCI cards 4.25 and later	—	—	x
WGB34x/352 8.58	—	x	—
WGB34x/352 8.61 or later	—	—	x
AP34x/35x 11.05 and earlier	—	x	—
AP34x/35x 11.06 and later[2]	—	x	x
BR352 11.06 and later[1]	—	x	x

1. Functionality in Draft 10 is equivalent to the functionality in Draft 11, the ratified draft of the 802.1X standard.

2. 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. Functionality in Draft 10 is equivalent to the functionality in Draft 11, the ratified draft of the 802.1X standard.

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.

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 6-16 for more information on the reset buttons in the web-browser interface.

Step 1   Connect a nine-pin, female DB-9 to RJ-45 serial cable to the RJ-45 serial port on the access point and to the COM port on a computer.

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

> ✎
>
> **Note**   These instructions describe HyperTerminal; other programs are similar.

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

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

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

- **9600** baud,

- **8** data bits,

- **No** parity,

- **1** stop bit, and

- **No** 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.

Channels, Power Levels, and Antenna Gains

This appendix lists the IEEE 802.11a and IEEE 802.11b channels supported by the world's regulatory domains as well as the maximum power levels and antenna gains allowed per domain.

The following topics are covered in this appendix:

Channels

Channels for IEEE 802.11a

The channel identifiers, channel center frequencies, and regulatory domains of each IEEE 802.11a 20-MHz-wide channel are listed in Table A-1.

Table A-1   Channels for IEEE 802.11a

Channel Identifier	Frequency in MHz	Regulatory Domains			
		Americas (-A)	Japan (-J)	Singapore (-S)	Taiwan (-T)
34	5170	-	X	-	-
36	5180	X	-	X	-
38	5190	-	X	-	-
40	5200	X	-	X	-
42	5210	-	X	-	-
44	5220	X	-	X	-
46	5230	-	X	-	-
48	5240	X	-	X	-
52	5260	X	-	-	X
56	5280	X	-	-	X
60	5300	X	-	-	X
64	5320	X	-	-	X
149	5745	-	-	-	-
153	5765	-	-	-	-
157	5785	-	-	-	-
161	5805	-	-	-	-

Note   All channel sets are restricted to indoor usage except the Americas (-A), which allows for indoor and outdoor use on channels 52 through 64 in the United States.

Channels for IEEE 802.11b

The channel identifiers, channel center frequencies, and regulatory domains of each IEEE 802.11b 22-MHz-wide channel are listed in Table A-2.

Table A-2 Channels for IEEE 802.11b

Channel Identifier	Frequency in MHz	Regulatory Domains				
		Americas (-A)	EMEA (-E)	Israel (-I)	China (-C)	Japan (-J)
1	2412	X	X	-	X	X
2	2417	X	X	-	X	X
3	2422	X	X	X	X	X
4	2427	X	X	X	X	X
5	2432	X	X	X	X	X
6	2437	X	X	X	X	X
7	2442	X	X	X	X	X
8	2447	X	X	X	X	X
9	2452	X	X	X	X	X
10	2457	X	X	-	X	X
11	2462	X	X	-	X	X
12	2467	-	X	-	-	X
13	2472	-	X	-	-	X
14	2484	-	-	-	-	X

Note Mexico is included in the Americas 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 complies with the regulatory standards of Mexico.

Note   France is included in the EMEA regulatory domain; however, only channels 10 through 13 can be used in France. Users are responsible for ensuring that the channel set configuration complies with the regulatory standards of France.

Maximum Power Levels and Antenna Gains

For IEEE 802.11a

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 A-3 indicates the maximum power levels and antenna gains allowed for each IEEE 802.11a regulatory domain.

Table A-3   Maximum Power Levels Per Antenna Gain for IEEE 802.11a

Regulatory Domain	Maximum Power Level (mW) with 6-dBi Antenna Gain
Americas (-A) (160 mW EIRP maximum on channels 36-48, 800 mW EIRP maximum on channels 52-64)	40
Japan (-J) (10 mW/MHz EIRP maximum)	40
Singapore (-S) (100 mW EIRP maximum)	20
Taiwan (-T) (800 mW EIRP maximum)	40

For IEEE 802.11b

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 A-4 indicates the maximum power levels and antenna gains allowed for each IEEE 802.11b regulatory domain.

Table A-4   Maximum Power Levels Per Antenna Gain for IEEE 802.11b

Regulatory Domain	Antenna Gain (dBi)	Maximum Power Level (mW)
Americas (-A) (4 watts EIRP maximum)	0	100
	2.2	100
	5.2	100
	6	100
	8.5	100
	12	100
	13.5	100
	21	20
EMEA (-E) (100 mW EIRP maximum)	0	100
	2.2	50
	5.2	30
	6	30
	8.5	5
	12	5
	13.5	5
	21	1

Cisco Aironet 1200 Series Access Point Software Configuration Guide ■

Table A-4   Maximum Power Levels Per Antenna Gain for IEEE 802.11b (continued)

Regulatory Domain	Antenna Gain (dBi)	Maximum Power Level (mW)
Israel (-I) (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 (-C) (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
Japan (-J) (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

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 3-9. 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