CISCO SYSTEMS

Cisco Aironet Access Point Software Configuration Guide

340 and 350 Series
Software Release 11.21

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-0657-06

CONTENTS

Preface xiii

Audience and Scope xiv

Organization xiv

Conventions xv

Related Publications xvi

Obtaining Documentation xvi

World Wide Web xvi

Documentation CD-ROM xvii

Ordering Documentation xvii

Documentation Feedback xvii

Obtaining Technical Assistance xviii

Cisco.com xviii

Technical Assistance Center xix

Cisco TAC Web Site xix

Cisco TAC Escalation Center xx

CHAPTER 1

Overview 1-1

Key Features 1-2

Management Options 1-3

Roaming Client Devices 1-3

Network Configuration Examples 1-4

Root Unit on a Wired LAN 1-4

Repeater Unit that Extends Wireless Range 1-5

Central Unit in an All-Wireless Network 1-6

CHAPTER 2 **Using the Management Interfaces 2-1**

Using the Web-Browser Interface 2-2
Using the Web-Browser Interface for the First Time 2-2
Using the Management Pages in the Web-Browser Interface 2-2
Navigating Using the Map Windows 2-4
Using the Command-Line Interface 2-5
Preparing to Use a Terminal Emulator 2-6
Connecting the Serial Cable 2-6
Setting Up the Terminal Emulator 2-7
Changing Settings with the CLI 2-8
Selecting Pages and Settings 2-9
Applying Changes to the Configuration 2-9
Navigating the CLI 2-10
Using a Telnet Session 2-10
Using SNMP 2-11
Supported MIBs 2-11

CHAPTER 3 **Configuration 3-1**

Basic Settings 3-2
Entering Basic Settings 3-3
System Name 3-3
Configuration Server Protocol 3-3
Default IP Address 3-4
Default IP Subnet Mask 3-4
Default Gateway 3-4
Radio Service Set ID (SSID) 3-4
Role in Radio Network 3-5
Radio Network Optimization (Optimize Radio Network For) 3-7
Radio Network Compatibility (Ensure Compatibility With) 3-7

SNMP Admin. Community 3-7
Filter Setup 3-8
Protocol Filtering 3-8
Creating a Protocol Filter 3-9
Enabling a Protocol Filter 3-12
MAC Address Filtering 3-13
Creating a MAC Address Filter 3-14
Radio Configuration 3-18
Entering Identity Information 3-18
Settings on the AP Radio Identification Page 3-19
Entering Radio Hardware Information 3-21
Settings on the AP Radio Hardware Page 3-22
Entering Advanced Configuration Information 3-30
Settings on the AP Radio Advanced Page 3-31
Ethernet Configuration 3-39
Entering Identity Information 3-39
Settings on the Ethernet Identification Page 3-40
Entering Ethernet Hardware Information 3-42
Settings on the Ethernet Hardware Page 3-43
Entering Advanced Configuration Information 3-44
Settings on the Ethernet Advanced Page 3-44
Server Setup 3-46
Entering Time Server Settings 3-47
Settings on the Time Server Setup Page 3-47
Entering Boot Server Settings 3-49
Settings on the Boot Server Setup Page 3-49
Entering Web Server Settings and Setting Up Access Point Help 3-53
Settings on the Web Server Setup Page 3-54
Entering Name Server Settings 3-56
Settings on the Name Server Setup Page 3-57

Entering FTP Settings 3-58
Settings on the FTP Setup Page 3-59
Routing Setup 3-60
Entering Routing Settings 3-60
Default Gateway 3-61
New Network Route Settings 3-61
Installed Network Routes list 3-61
Association Table Display Setup 3-62
Association Table Filters Page 3-62
Settings on the Association Table Filters Page 3-63
Association Table Advanced Page 3-66
Settings on the Association Table Advanced Page 3-67
Event Notification Setup 3-69
Event Display Setup Page 3-69
Settings on the Event Display Setup Page 3-69
Event Handling Setup Page 3-72
Settings on the Event Handling Setup Page 3-74
Event Notifications Setup Page 3-76
Settings on the Event Notifications Setup Page 3-77

CHAPTER 4 **Security Setup 4-1**

Security Overview 4-2
Levels of Security 4-2
Encrypting Radio Signals with WEP 4-3
Additional WEP Security Features 4-3
Network Authentication Types 4-4
Combining MAC-Based, EAP, and Open Authentication 4-8
Protecting the Access Point Configuration with User Manager 4-9
Setting Up WEP 4-9

Using SNMP to Set Up WEP 4-12
Enabling Additional WEP Security Features 4-13
Enabling Message Integrity Check (MIC) 4-14
Enabling Temporal Key Integrity Protocol (TKIP) 4-16
Enabling Broadcast WEP Key Rotation 4-17
Setting Up Open or Shared Key Authentication 4-19
Setting Up EAP Authentication 4-19
Enabling EAP on the Access Point 4-20
Enabling EAP in Cisco Secure ACS 4-25
Setting a Session-Based WEP Key Timeout 4-26
Setting up a Repeater Access Point as a LEAP Client 4-27
Setting Up MAC-Based Authentication 4-29
Enabling MAC-Based Authentication on the Access Point 4-29
Authenticating Client Devices Using MAC Addresses or EAP 4-34
Enabling MAC-Based Authentication in Cisco Secure ACS 4-35
Summary of Settings for Authentication Types 4-37
Setting Up Backup Authentication Servers 4-40
Setting Up Administrator Authorization 4-41
Creating a List of Authorized Management System Users 4-42

CHAPTER 5 **Network Management 5-1**

Using the Association Table 5-2
Browsing to Network Devices 5-2
Setting the Display Options 5-3
Using Station Pages 5-3
Information on Station Pages 5-5
Performing Pings and Link Tests 5-8
Clearing and Updating Statistics 5-10
Deauthenticating and Disassociating Client Devices 5-11

Using the Network Map Window 5-11
Using Cisco Discovery Protocol 5-13
Settings on the CDP Setup Page 5-14
MIB for CDP 5-14
Assigning Network Ports 5-14
Settings on the Port Assignments Page 5-16
Enabling Wireless Network Accounting 5-16
Settings on the Accounting Setup Page 5-17
Accounting Attributes 5-19

CHAPTER 6 **Managing Firmware and Configurations 6-1**
Updating Firmware 6-2
Updating with the Browser from a Local Drive 6-2
Full Update of the Firmware Components 6-3
Selective Update of the Firmware Components 6-4
Updating from a File Server 6-5
Full Update of the Firmware Components 6-5
Selective Update of the Firmware Components 6-7
Distributing Firmware 6-8
Distributing a Configuration 6-9
Downloading, Uploading, and Resetting the Configuration 6-11
Downloading the Current Configuration 6-12
Uploading a Configuration 6-12
Uploading from a Local Drive 6-12
Uploading from a File Server 6-13
Resetting the Configuration 6-15
Restarting the Access Point 6-16

CHAPTER 7 **Management System Setup 7-1**

SNMP Setup 7-2

Settings on the SNMP Setup Page 7-2

Using the Database Query Page 7-3

Settings on the Database Query Page 7-4

Changing Settings with the Database Query Page 7-4

Console and Telnet Setup 7-5

Settings on the Console/Telnet Page 7-5

CHAPTER 8 **Special Configurations 8-1**

Setting Up a Repeater Access Point 8-1

Using Hot Standby Mode 8-6

CHAPTER 9 **Diagnostics and Troubleshooting 9-1**

Using Diagnostic Pages 9-2

Radio Diagnostics Page 9-2

Antenna Alignment Test 9-3

Carrier Test 9-5

Network Ports Page 9-6

Identifying Information and Status 9-8

Data Received 9-8

Data Transmitted 9-9

Ethernet Port Page 9-10

AP Radio Page 9-13

Event Log Page 9-17

Display Settings 9-17

Log Headings 9-18

Saving the Log 9-18

Event Log Summary Page 9-19

Using Command-Line Diagnostics 9-20
Entering Diagnostic Commands 9-21
Diagnostic Command Results 9-22
:eap_diag1_on 9-22
:eap_diag2_on 9-23
:vxdiag_arpshow 9-23
:vxdiag_checkstack 9-25
:vxdiag_hostshow 9-26
:vxdiag_i 9-27
:vxdiag_ipstatshow 9-28
:vxdiag_memshow 9-29
:vxdiag_muxshow 9-30
:vxdiag_routeshow 9-31
:vxdiag_tcpstatshow 9-32
:vxdiag_udpstatshow 9-33
Tracing Packets 9-33
Reserving Access Point Memory for a Packet Trace Log File 9-33
Tracing Packets for Specific Devices 9-34
Tracing Packets for Ethernet and Radio Ports 9-35
Viewing Packet Trace Data 9-36
Packets Stored in a Log File 9-37
Packets Displayed on the CLI 9-38
Checking the Top Panel Indicators 9-38
Finding an Access Point by Blinking the Top Panel Indicators 9-41
Checking Basic Settings 9-41
SSID 9-41
WEP Keys 9-41
EAP Authentication Requires Matching 802.1x Protocol Drafts 9-42
Resetting to the Default Configuration 9-44
Steps for Firmware Versions 11.07 or Later 9-44

Steps for Firmware Versions 11.06 or Earlier 9-46
Determining the Boot-Block Version 9-46
Reconfiguration Steps for Boot Block Version 1.01 or Earlier 9-47
Reconfiguration Steps for Boot Block Version 1.02 or Later 9-49

APPENDIX A **Menu Tree A-1**

APPENDIX B **Protocol Filter Lists B-1**

APPENDIX C **Channels, Power Levels, and Antenna Gains C-1**
Channels C-2
Maximum Power Levels and Antenna Gains C-3

INDEX INDEX

Preface

The *Cisco Aironet Access Point Software Configuration Guide* describes how to configure Cisco Aironet 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 change the configuration of 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, "Menu Tree," provides an overview of the management system's menu organization.

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

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

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 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 Access Points* describes how to attach cables, power on, and assign an IP address and default gateway for the access point.
- *Cisco Aironet Access Point Hardware Installation Guide* describes the access point's hardware features, its physical and performance characteristics, and how to install the access point.
- *Release Notes for Cisco Aironet 340 and 350 Series Access Points and 350 Series Bridges* describes features and caveats for access points running firmware release 11.20.
- *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.

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.

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 1-3
- Roaming Client Devices, page 1-3
- Network Configuration Examples, page 1-4

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.

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

- 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), Temporal Key Integrity Protocol (TKIP, also known as 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.

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

- Use 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.

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

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.

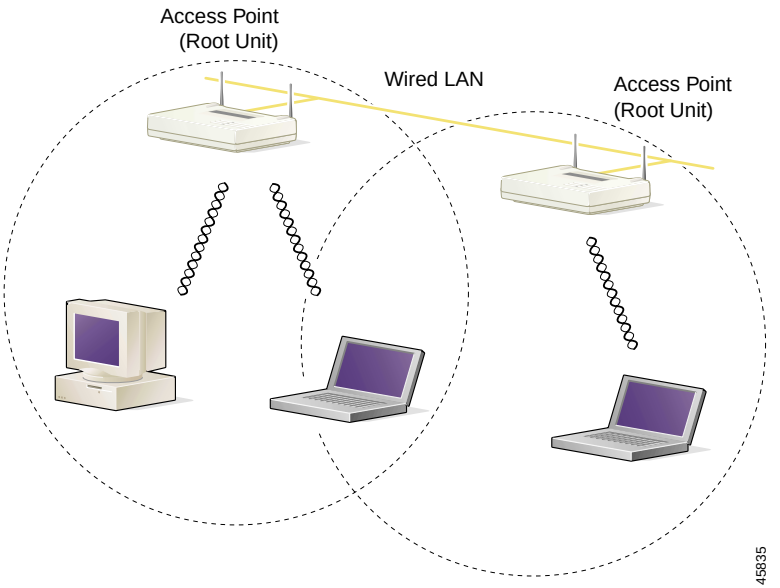
Network Configuration Examples

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

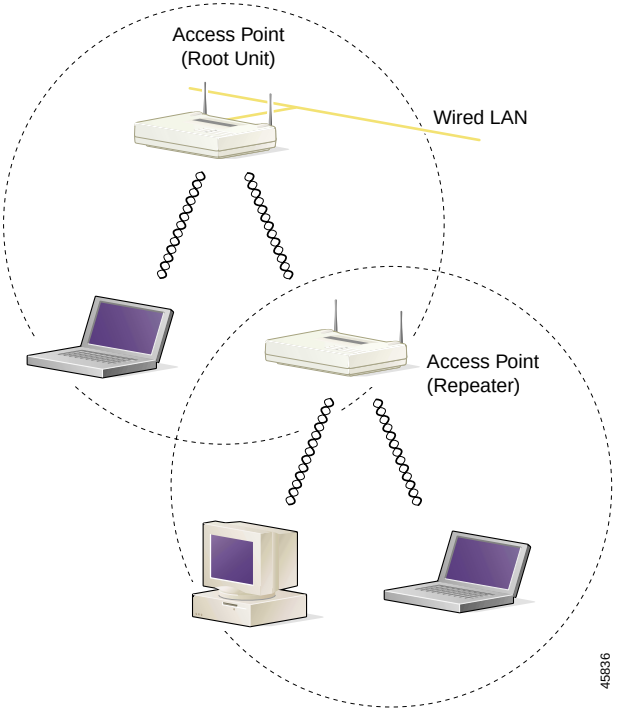


Repeater Unit that Extends Wireless Range

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. 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 an access point as a repeater.

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

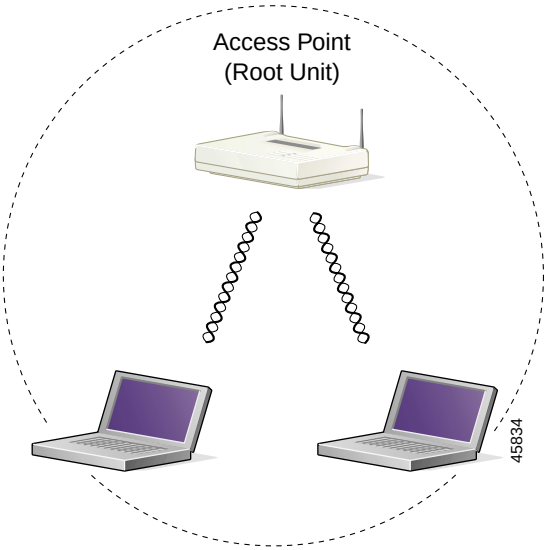
Figure 1-2 Access Point as Repeater



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



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, page 2-2
- Using the Command-Line Interface, page 2-5
- Using SNMP, page 2-11

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 350 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.

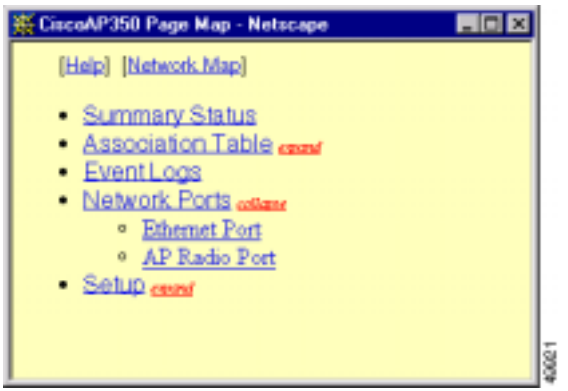
Navigating Using the Map Windows

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.

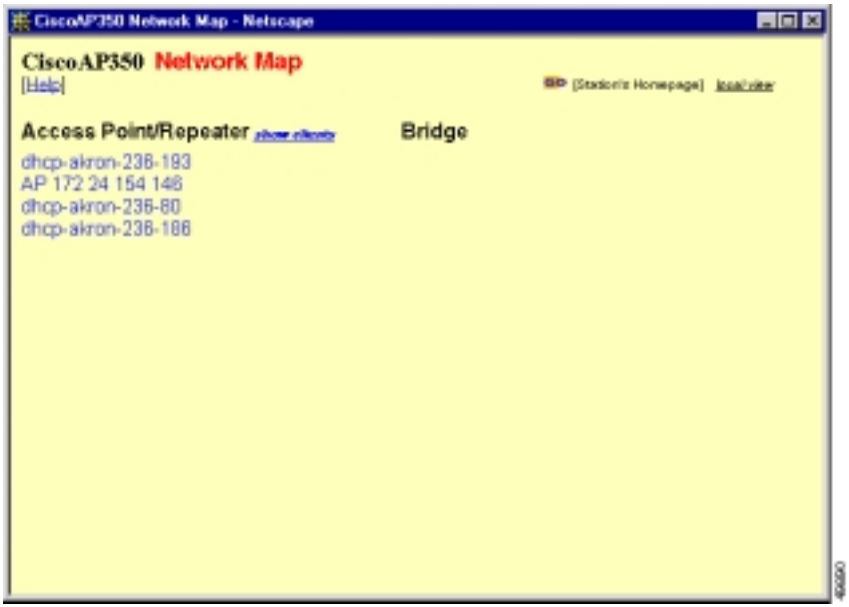
To display the sub-pages for each main page, click the bullet next to a main page link (Microsoft Internet Explorer), or click **expand** next to a main page link (Netscape Communicator). In Figure 2-1, the sub-pages for the Network Ports page are expanded.

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, straight-through DB-9 serial cable to the RS-232 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, Xon/Xoff 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 nine-pin, male-to-female, straight-through serial cable to the COM port on a computer and to the RS-232 serial port on the access point. Figure 2-3 shows the serial port on an access point with a plastic case, and Figure 2-4 shows the location of the serial port on an access point with a metal case.

Figure 2-3 Connecting the Serial Cable on Access Point with Plastic Case

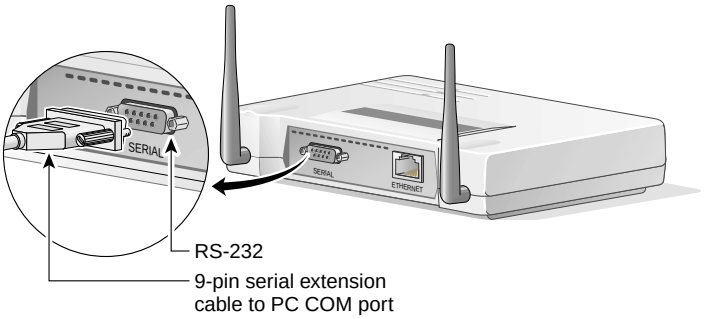
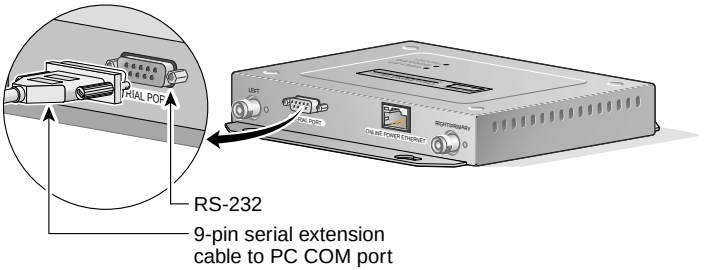


Figure 2-4 Connecting the Serial Cable on Access Point with Metal Case



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: Xon/Xoff

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, and Figure 2-5 shows a CLI page example.

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.
: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*.

Figure 2-5 CLI Page Example

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**.

Navigating the CLI

The organization of the CLI pages is identical to the web-browser pages. Consult Appendix A, "Menu Tree," for a complete organizational overview of the management pages.

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.

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:

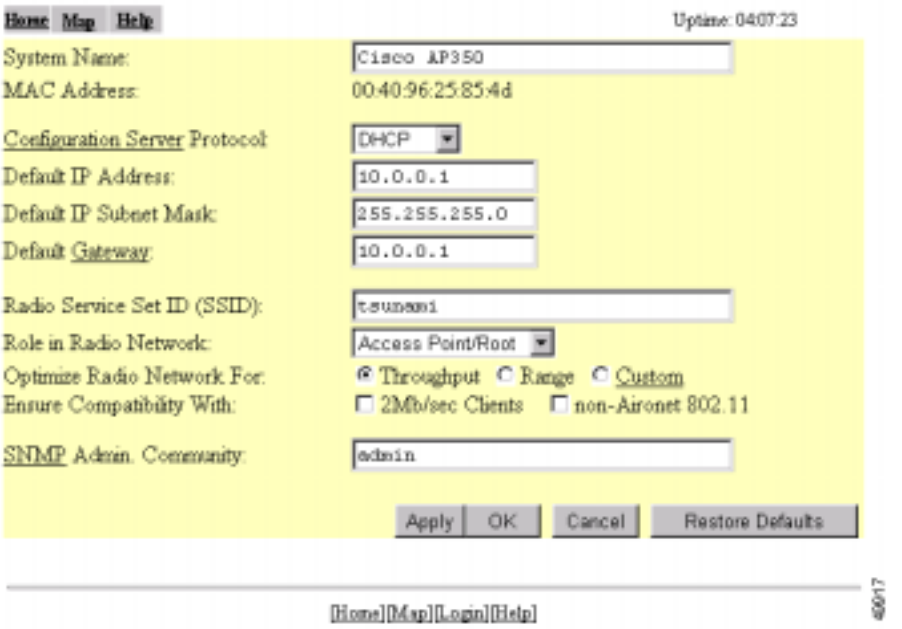
- Basic Settings, page 3-2
- Filter Setup, page 3-8
- Radio Configuration, page 3-18
- Ethernet Configuration, page 3-39
- Server Setup, page 3-46
- Routing Setup, page 3-60
- Association Table Display Setup, page 3-62
- Event Notification Setup, page 3-69

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. Figure 3-1 shows the Express Setup page.

Figure 3-1 The 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
- 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.

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)

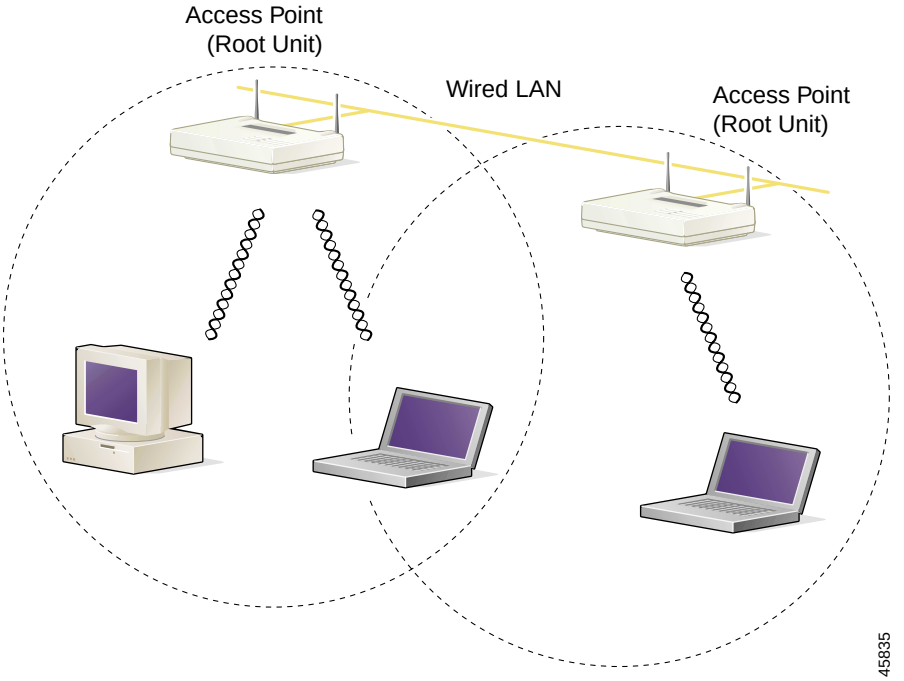
The SSID is a unique identifier that client devices use to associate with the access point. The SSID helps client devices distinguish between multiple wireless networks in the same vicinity. Several access points on a network or sub-network can share an SSID. The SSID can be any alphanumeric, case-sensitive entry from two to 32 characters long.

Role in Radio Network

Use this pull-down menu to select the role of the access point on your network. 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.

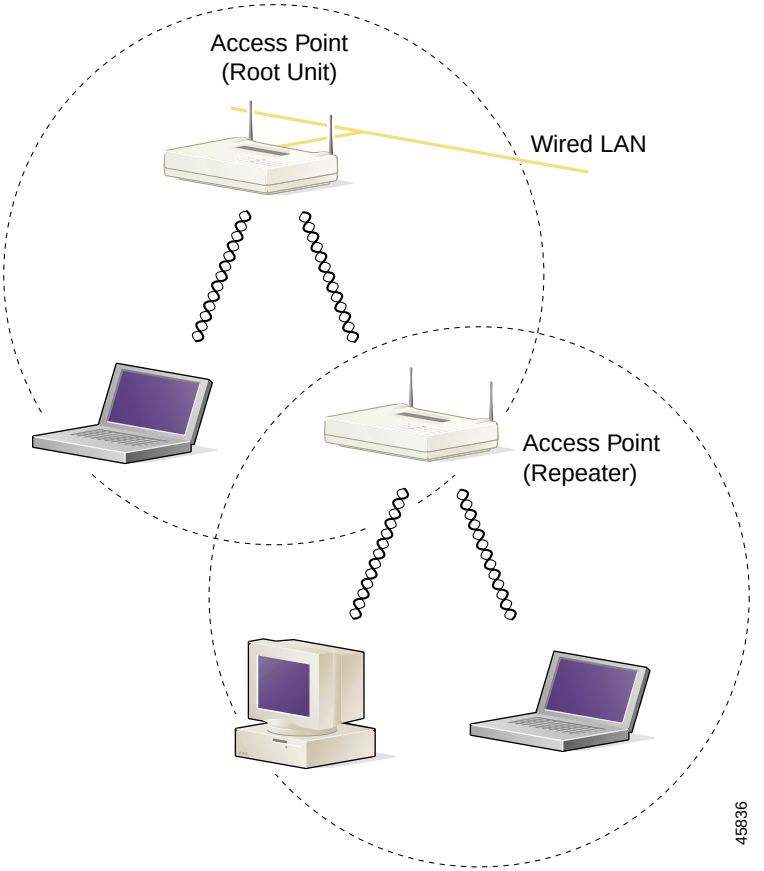
Figure 3-2 Root-Unit Access Points



- Repeater Access Point—An access point that transfers data between a client and another access point or repeater. Use this setting for access points not connected to the wired LAN. 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.

- 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.

- 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:

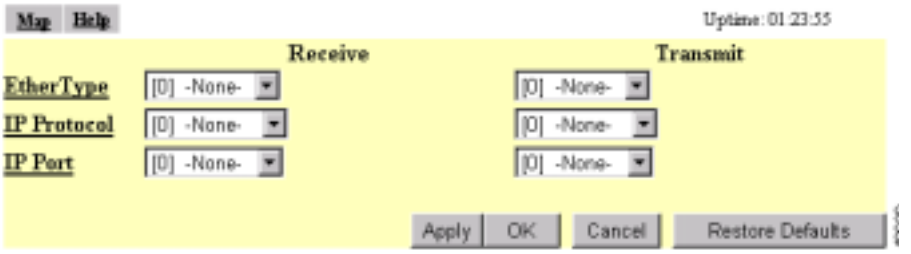
- Protocol Filtering, page 3-8
- MAC Address Filtering, page 3-13

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.

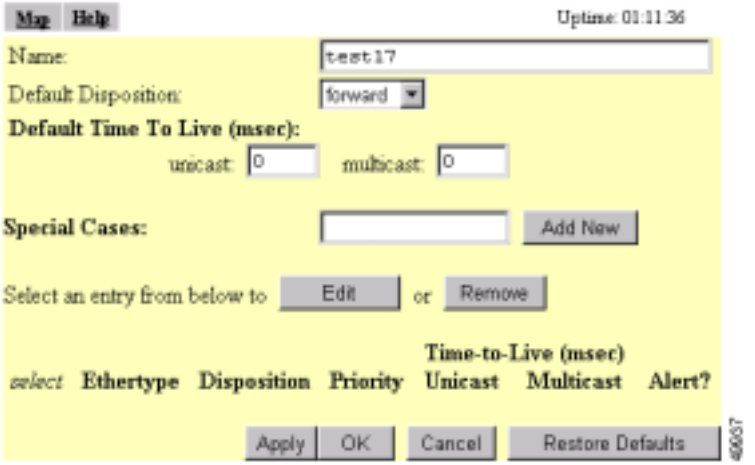
Figure 3-5 Filters Page

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



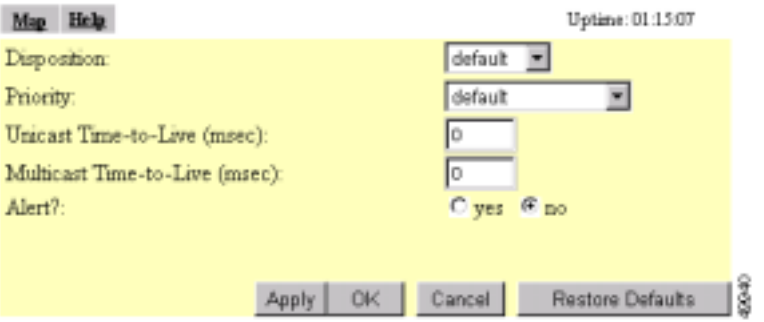
Step 6 Select **forward** or **block** from the Default Disposition pull-down menu. This setting is the default action for the protocols you include in the filter set. You can override this setting for specific protocols.

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 3-9 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.

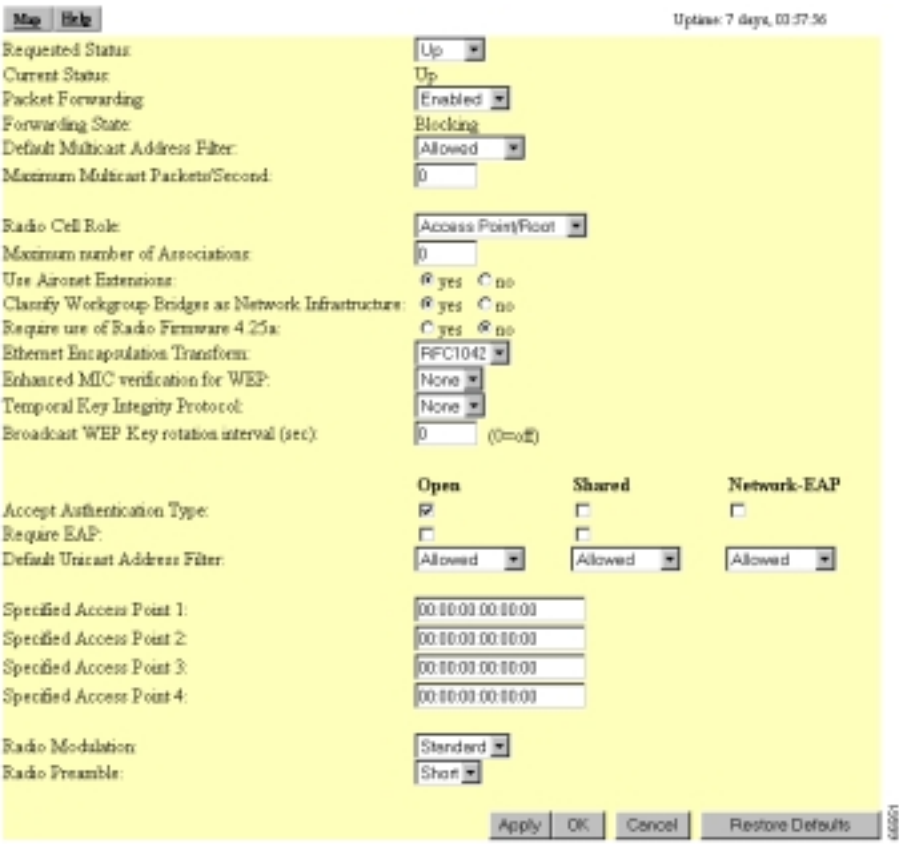
Step 4 Click **Add**. The MAC address appears in the Existing MAC Address Filters list. To remove the MAC address from the list, select it and click **Remove**.

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.

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

Step 6 Click **Advanced** in the AP Radio row of the Network Ports section at the bottom of the Setup page. The AP Radio Advanced page appears. Figure 3-9 shows the AP Radio Advanced page.

Figure 3-9 AP Radio Advanced Page



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 3-66 for information on setting a monitoring timeout for each device class.

Radio Configuration

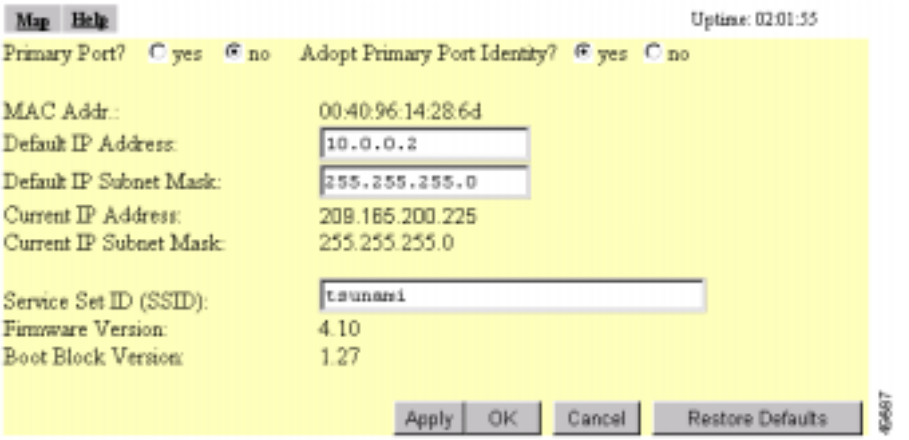
This section describes how to configure the access point's radio. You use the AP Radio pages in the management system to set the radio configuration. The radio pages include:

- AP Radio Identification—Contains the basic locating and identity information for the access point Radio port. See the "Entering Identity Information" section on page 3-18 for instructions on using the AP Radio Identification page.
- AP Radio Hardware—Contains settings for the access point's SSID, data rates, transmit power, antennas, radio channel, and operating thresholds. See the "Entering Radio Hardware Information" section on page 3-21 for instructions on using the AP Radio Hardware page.
- AP Radio Advanced—Contains settings for the operational status of the access point's radio port. You can also use this page to make temporary changes in port status to help with troubleshooting network problems. See the "Entering Advanced Configuration Information" section on page 3-30 for instructions on using the AP Radio Advanced page.
- AP Radio Port—Lists key information on the access point's radio port.

Entering Identity Information

You use the AP Radio Identification page to enter basic locating and identity information for the access point radio. Figure 3-10 shows the AP Radio Identification page.

Figure 3-10 The AP Radio Identification Page



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 the AP Radio row under Network Ports.

Settings on the AP Radio Identification Page

The AP Radio Identification page contains 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, its current IP address, its current IP subnet mask, its firmware version, and its boot block version.

Primary Port Settings

Two options allow you to designate the access point's 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. 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

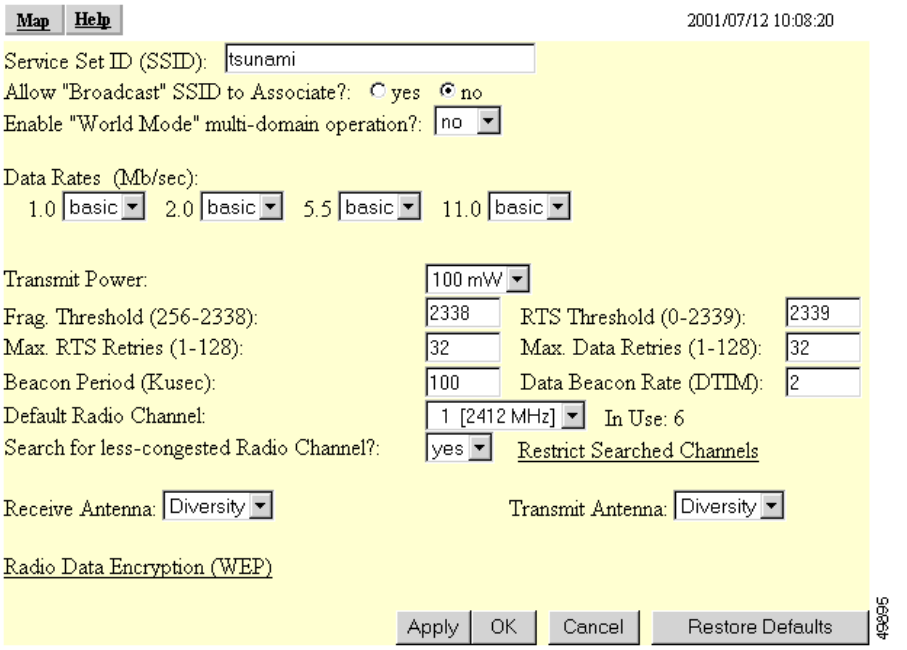
Use this field if the radio is set up as a repeater and authenticates to the network using LEAP. When the radio authenticates using LEAP, the access point uses this password for authentication.

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 page to assign settings related to the access point's radio hardware. Figure 3-11 shows the AP Radio Hardware page.

Figure 3-11 The AP Radio Hardware Page



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

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Hardware** in the AP Radio row 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)
- 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. 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 with the access point.

- 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 with the access point.
- 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 with the access point. With no selected, the SSID used by the client device must match exactly the access point'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

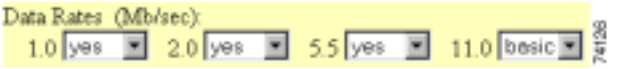
You use the data rate settings to choose the data rates the access point uses for data transmission. The rates are expressed in megabits per second.

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 of four rates (1, 2, 5.5, and 11 megabits per second), a drop-down menu lists three options:

- Basic (default)—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.

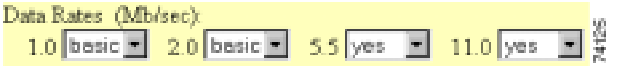
You can use the Data Rate settings to set up an access point to serve client devices operating at specific data rates. For example, to set up the access point for 11 megabits per second (Mbps) service only, select **Basic** for 11 and select **Yes** for the other data rates. Figure 3-12 shows the Data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



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 four data rates are set to basic. When you select **Optimize Radio Network For Range** on the Express Setup page, the 1.0 data rate is set to basic, and the other data rates are set to Yes.

Transmit Power

This setting determines the power level of radio transmission.

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 on 350 series access points include 1, 5, 20, 50, and 100 milliwatts. The settings in the drop-down menu on 340 series access points include 1, 5, and 30 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 2, its default setting, then the access point sends a beacon containing a DTIM every 200 Kμsecs. One Kμsec equals 1,024 microseconds.

Radio Channel

The factory setting for Cisco wireless LAN systems is Radio Channel 6 transmitting at 2437 MHz. To overcome an interference problem, other channel settings are available from the drop-down menu of 11 channels ranging 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.

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

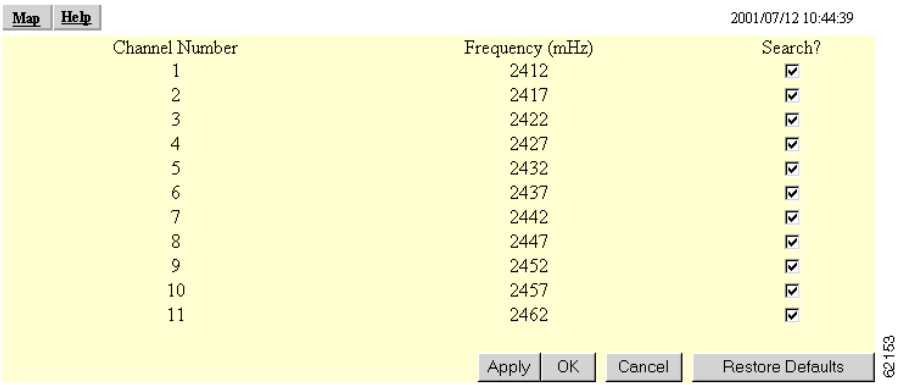
When you select **yes** from the Search for less-congested radio channel pull-down menu, the access point scans for the radio channel that is least busy and selects that channel for use. The access point scans at power-up and when the radio settings are changed.

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.

Figure 3-14 AP Radio Restrict Searched Channels Page



The page lists all the channels in the access point's regulatory domain. Click the **Search** check boxes beside the channels to include or exclude 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:

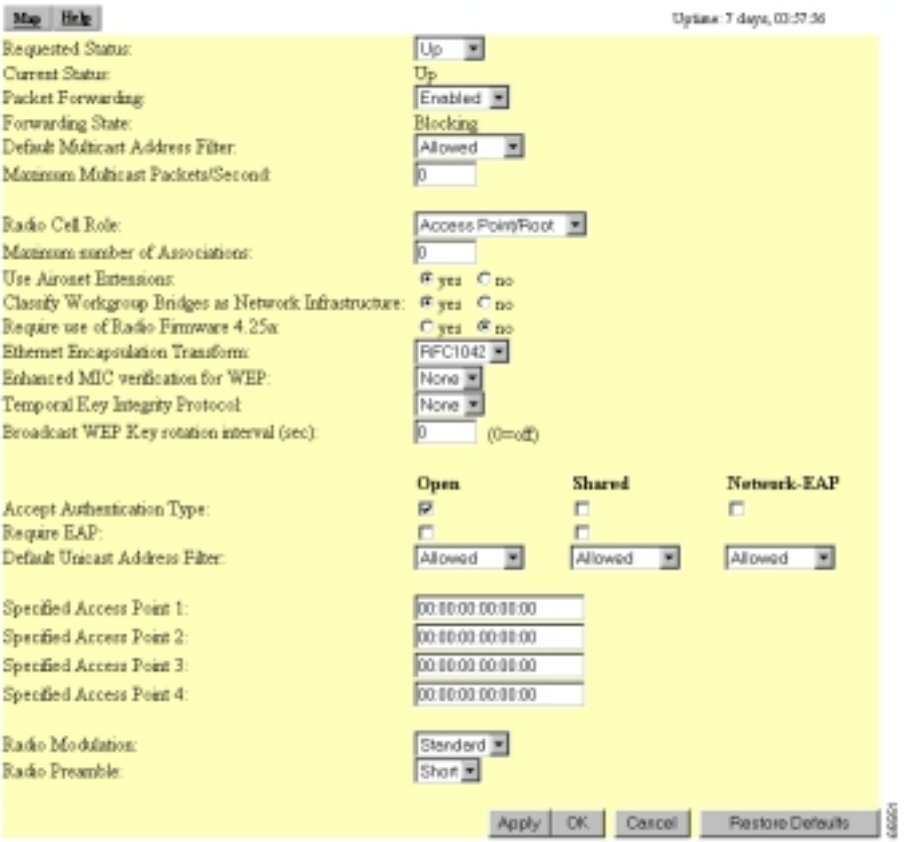
- Diversity—This default setting tells the access point to use the antenna that receives the best signal. If your access point has two fixed (non-removeable) antennas, you should use this setting for both receive and transmit.
- Right—If your access point has removeable antennas and you install a high-gain 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 page to assign special configuration settings for the access point's radio. Figure 3-15 shows the AP Radio Advanced page.

Figure 3-15 AP Radio Advanced Page



Follow this link path to reach 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.

Settings on the AP Radio Advanced Page

The AP Radio Advanced page contains 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)
- Bridge Spacing
- 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 access point's 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 3-14 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.

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 access point's radio within its radio coverage area (cell). This setting determines how the access point's 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 access point 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 access point. 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.
- 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, or 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. TKIP 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 TKIP.

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 key hashing 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.

Bridge Spacing

This setting is used on bridges to adjust the bridges' timeout values to account for the time required for radio signals to travel from bridge to bridge. This setting is not used on access points.

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 3-14 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

You 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.

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.

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.

Ethernet Configuration

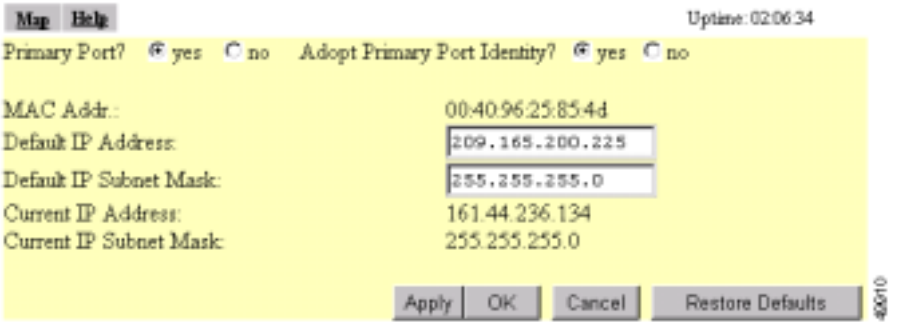
This section describes how to configure the access point's Ethernet port. You use the Ethernet pages in the management system to set the Ethernet port configuration. The Ethernet pages include:

- 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, 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.

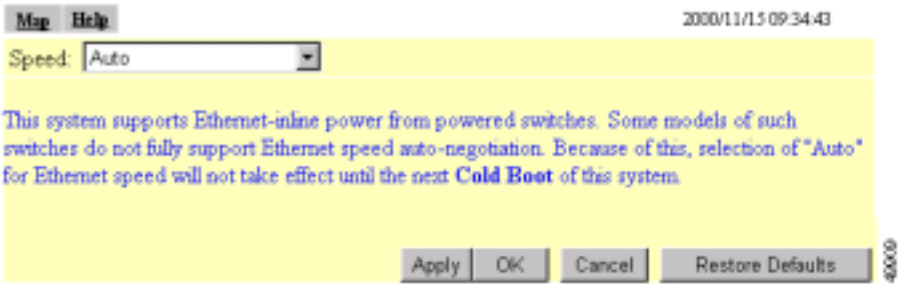
The current IP subnet mask displayed under the setting shows the IP subnet mask currently assigned to the access point. This is the same subnet mask as the default subnet mask unless DHCP or BOOTP is enabled. If DHCP or BOOTP is enabled, this is the subnet mask used by the server.

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 350 series 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 3-14 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.

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.

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:

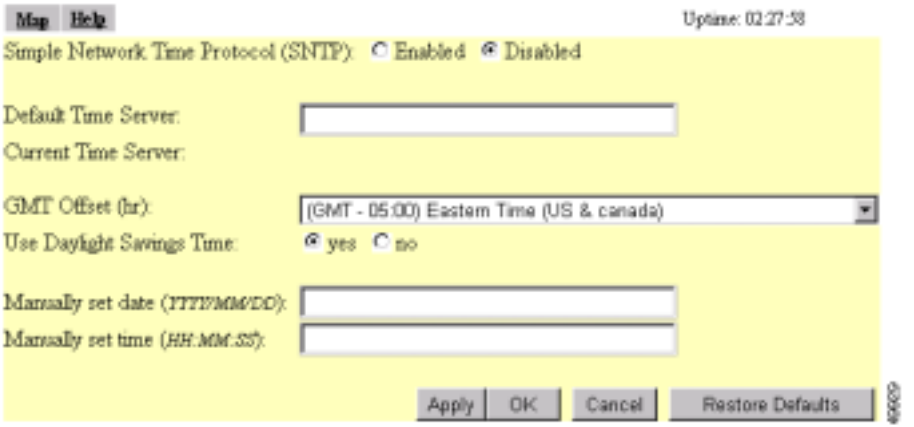
- Entering Time Server Settings, page 3-47
- Entering Boot Server Settings, page 3-49
- Entering Web Server Settings and Setting Up Access Point Help, page 3-53
- Entering Name Server Settings, page 3-56
- Entering FTP Settings, page 3-58

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

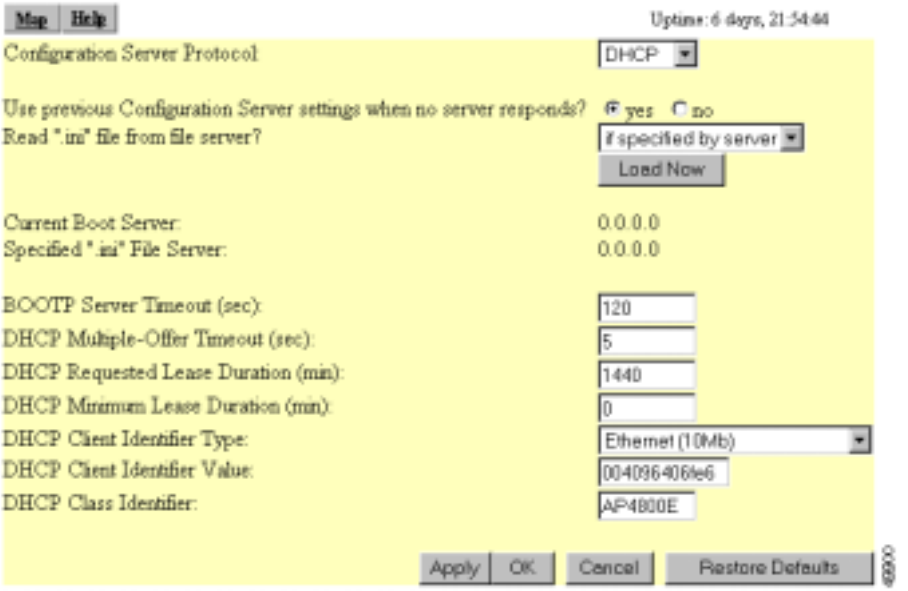
Enter the current date and time in the entry fields to override the time server or to set the date and time if no server is available.

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.

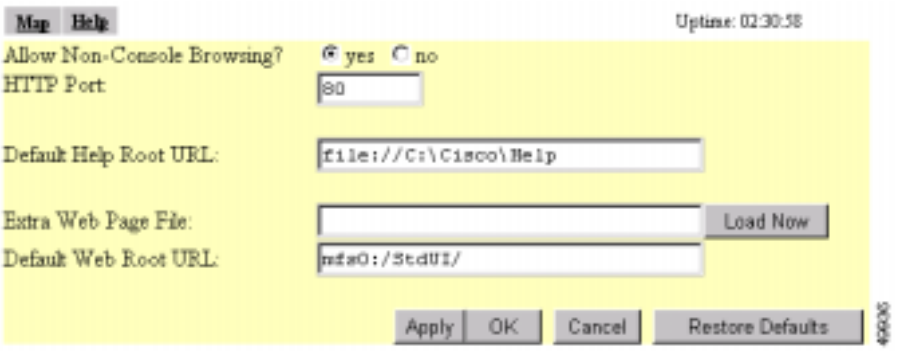
DHCP Class Identifier

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. The online help files are provided on the access point and bridge CD in the Help directory. You can point to the help files in one of four 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

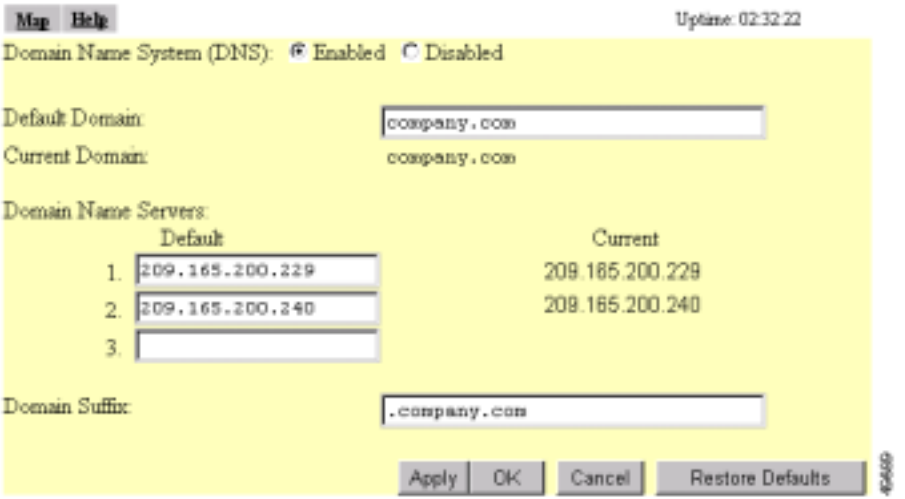
This setting points to the access point management system's HTML pages. If you create alternative HTML pages, you should change this setting to point to the alternative pages. The default setting is:

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

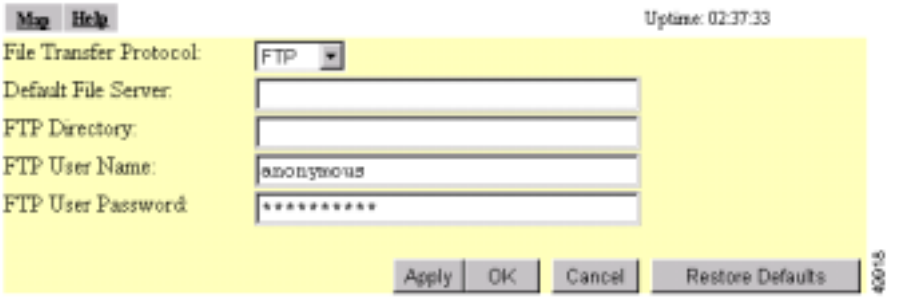
In this entry field, enter the portion of the full domain name that you would like omitted from access point displays. For example, in the domain “mycompany.com” the full name of a computer might be

"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.

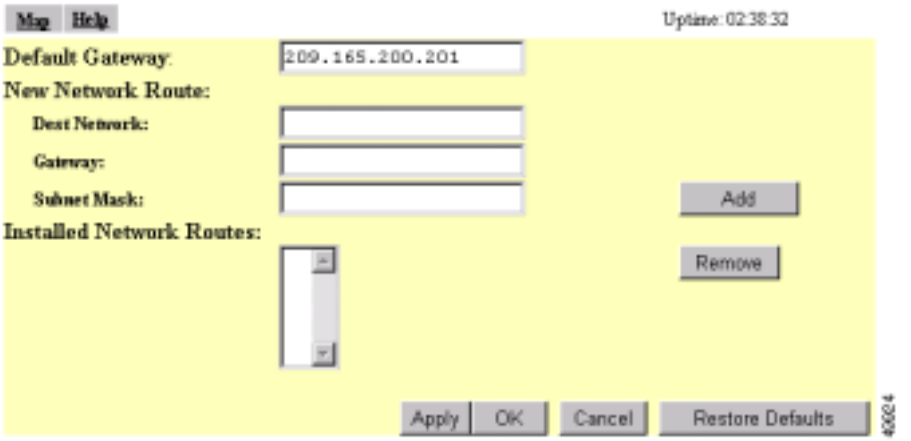
FTP User Password

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.

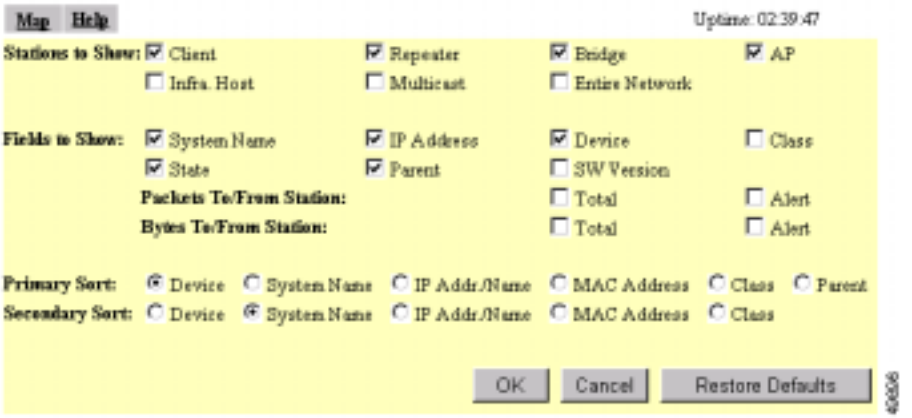
Association Table Display Setup

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 3-72 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.

Note The PSPF feature is available in firmware versions 11.08 and later, which are available on Cisco.com. You can download Cisco Aironet firmware releases at http://www.cisco.com/public/sw-center/sw-wireless.shtml.

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.

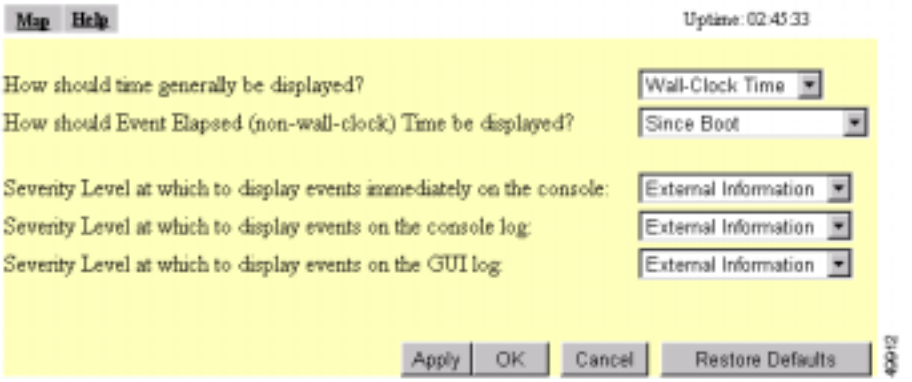
Event Notification Setup

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 3-72 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.

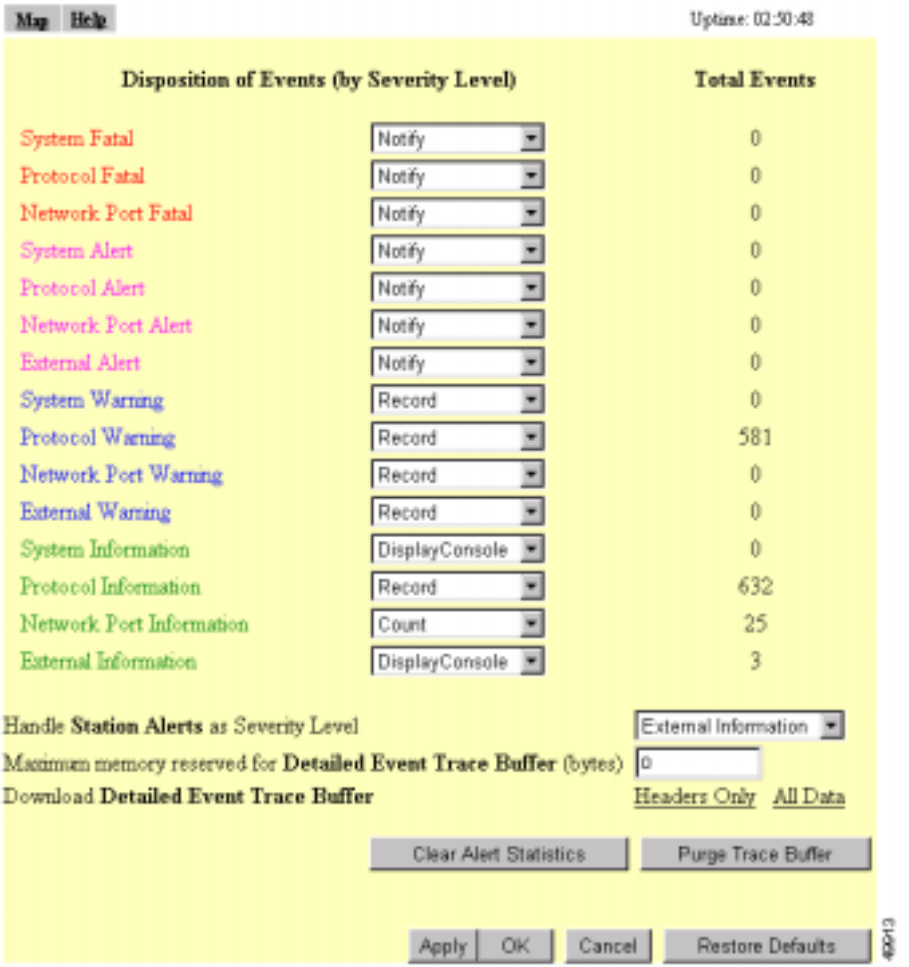
These selections affect display of events only. They are used to filter information, not to remove it from the Event Log. To remove information from the Event Log, click **Purge Log** on the Event Log page.

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 3-71 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.

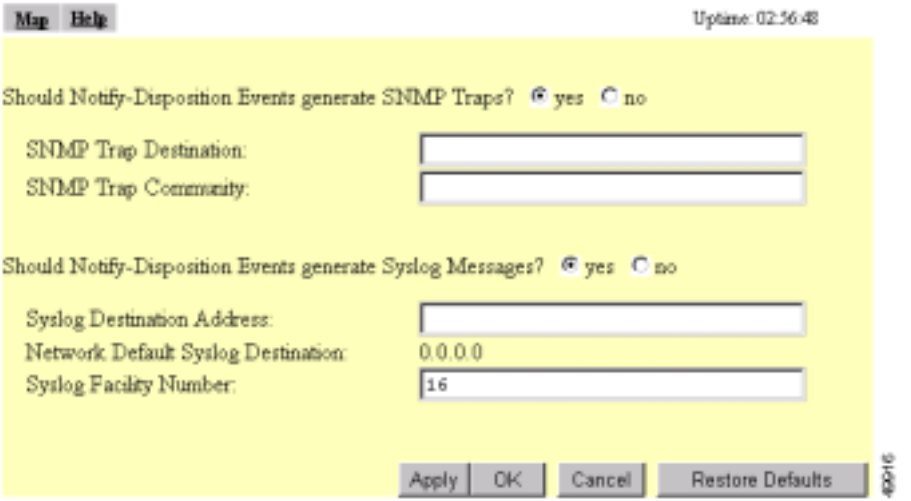
Event Notifications Setup Page

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 3-72 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 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, page 4-2
- Setting Up WEP, page 4-9
- Enabling Additional WEP Security Features, page 4-13
- Setting Up Open or Shared Key Authentication, page 4-19
- Setting Up EAP Authentication, page 4-19
- Setting Up MAC-Based Authentication, page 4-29
- Summary of Settings for Authentication Types, page 4-37
- Setting Up Backup Authentication Servers, page 4-40
- Setting Up Administrator Authorization, page 4-41

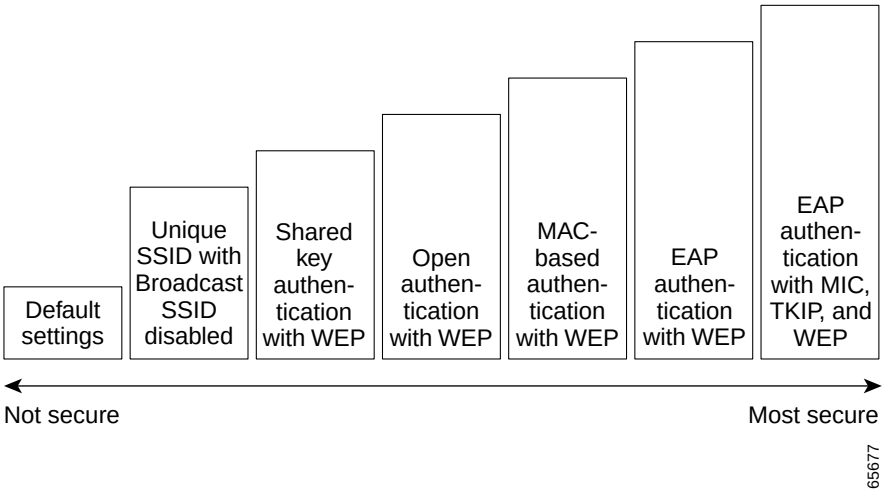
Security Overview

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.

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 4-17 for instructions on enabling broadcast key rotation.

Note The MIC, TKIP, and broadcast key rotation features are available in firmware versions 11.10T and later, which are available on Cisco.com. You can download Cisco Aironet firmware releases at http://www.cisco.com/public/sw-center/sw-wireless.shtml.

Network Authentication Types

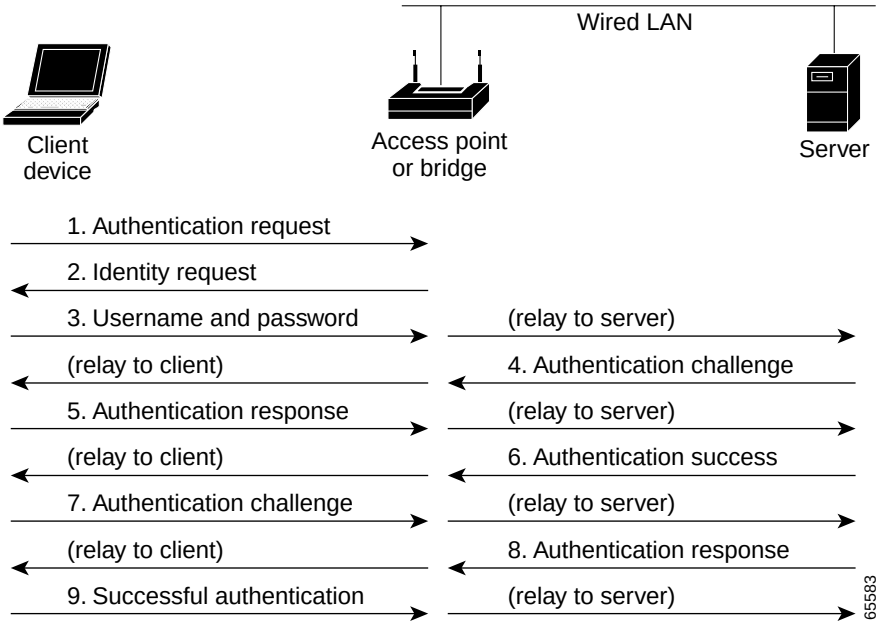
Before a wireless client device can communicate on your network through the access point, it must authenticate to the access point and to your network. The access point uses four authentication mechanisms or types and can use more than one at the same time:

- 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.

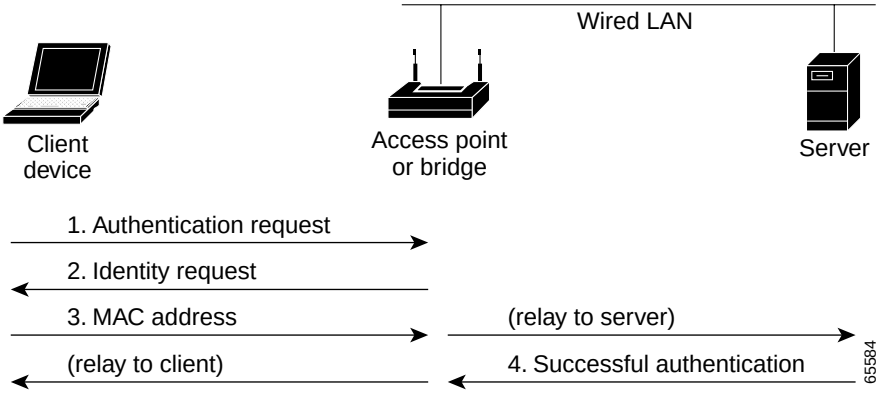
There is more than one type of EAP authentication, but the access point behaves the same way for each type: it relays authentication messages from the wireless client device to the RADIUS server and from the RADIUS server to the wireless client device. See the "Setting Up EAP Authentication" section on page 4-19 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.

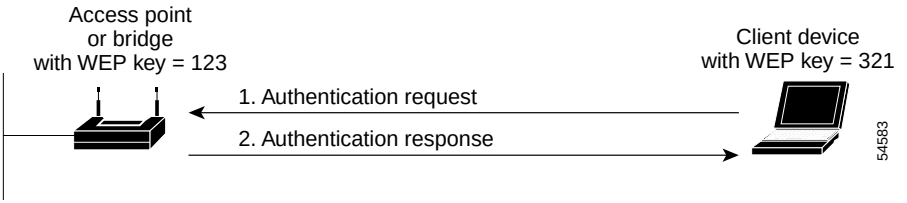
Figure 4-3 Sequence for MAC-Based Authentication



- 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

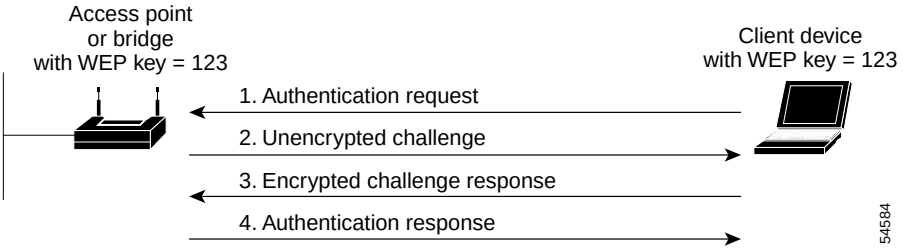


- Shared key—Cisco provides shared key authentication to comply with the IEEE 802.11b standard. However, because of shared key's security flaws, we recommend that you avoid using it.

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.

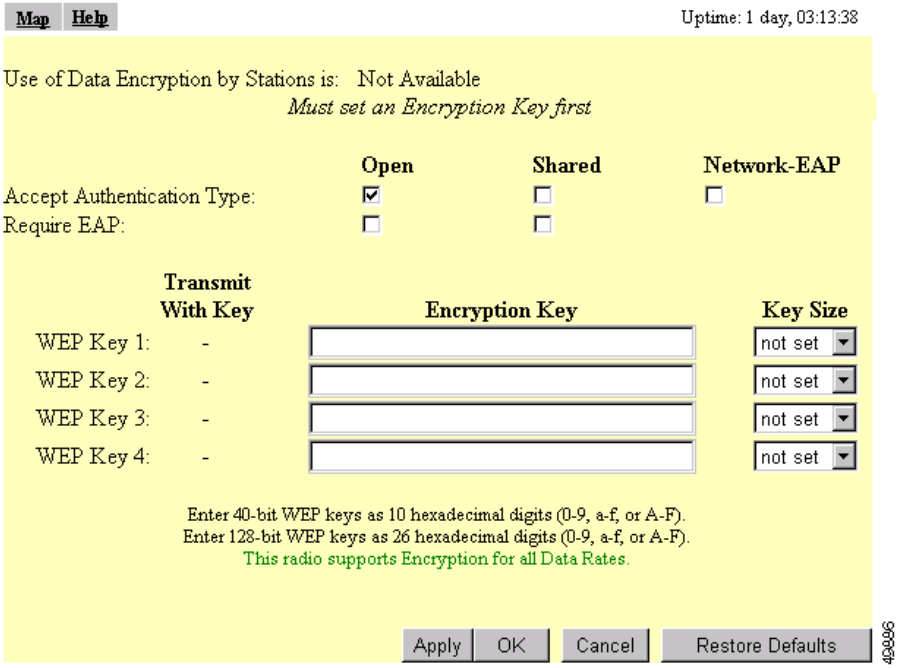
Protecting the Access Point Configuration with User Manager

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 page to set up WEP. You also use the AP Radio Data Encryption page to select an authentication type for the access point. 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)**.

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. If MIC is also enabled on the access point, the key must also 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

	Access Point		Associated Device	
Key Slot	**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.

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 2-11 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

Note The MIC, TKIP, and broadcast key rotation features are available in firmware versions 11.10T and later, which are available on Cisco.com. You can download Cisco Aironet firmware releases at http://www.cisco.com/public/sw-center/sw-wireless.shtml.

Enabling Message Integrity Check (MIC)

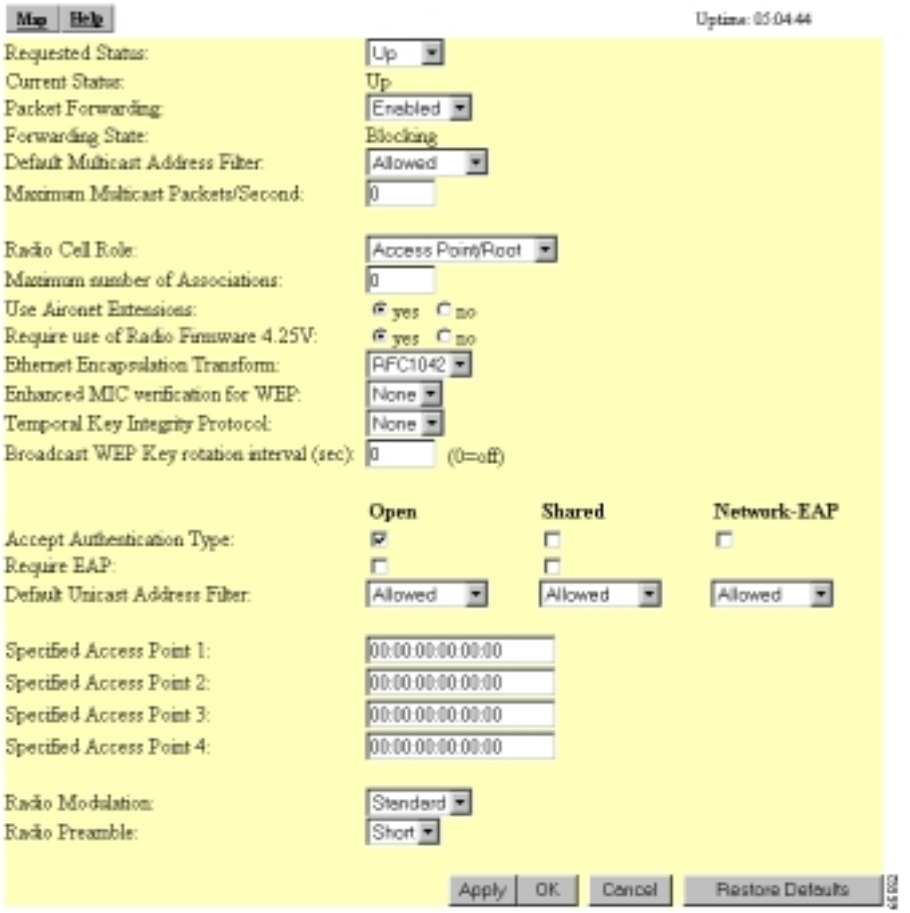
MIC prevents attacks on encrypted packets called *bit-flip* attacks. During a bit-flip attack, an intruder intercepts an encrypted message, alters it slightly, and retransmits it, and the receiver accepts the retransmitted message as legitimate. The MIC, implemented on both the access point and all associated 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 To use MIC, the Use Aironet Extensions setting on the AP Radio Advanced page must be set to yes (the default setting).

Use the AP Radio Advanced page to enable MIC. Figure 4-7 shows the AP Radio Advanced page.

Figure 4-7 AP Radio Advanced Page



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.

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 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.

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 might 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.

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.

Tip Broadcast key rotation and TKIP (WEP key hashing) provide similar protection. If you enable TKIP, you might not need to enable key rotation.

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.

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. Figure 4-6 shows the AP Radio Data Encryption page.

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 4-19 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:

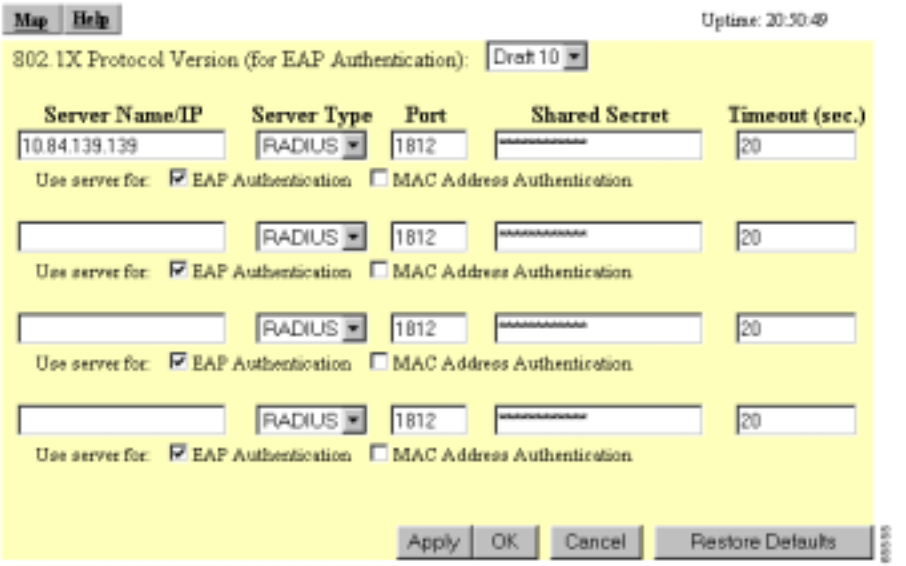
- Enabling EAP on the Access Point

- 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 page to set up and enable EAP authentication. Figure 4-6 shows the AP Radio Data Encryption page. 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 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—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 the radio firmware versions 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)** to browse to the 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 the access point.

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 (WEP key hashing) 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 your access point as a repeater (an access point not connected to the wired LAN), you can set up the repeater access point to authenticate to your network like other wireless client devices. After you provide a network username and password for the repeater access point, 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 access point:

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

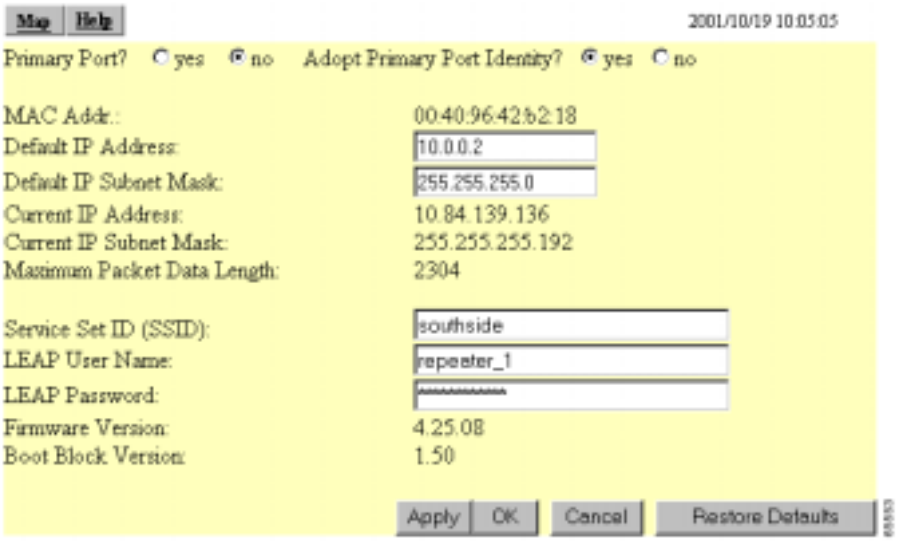
Step 2 Follow this link path to browse to the AP Radio Identification page:

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

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

Figure 4-9 shows the AP Radio Identification page.

Figure 4-9 AP Radio Identification Page



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

Step 4 Enter the network password you set up for the access point 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 and on a server used for MAC-based authentication.

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.