



Cisco IOS Software Configuration Guide for Cisco Aironet 1300 Series Outdoor Access Point/Bridge

Cisco IOS Release 12.3(7)JA
August 2005

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-7080-01



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

Cisco IOS Software Configuration Guide for Cisco Aironet 1300 Series Outdoor Access Point/Bridge

Copyright © 2005 Cisco Systems, Inc. All rights reserved.



Preface	xvii
Audience	xvii
Purpose	xvii
Organization	xvii
Conventions	xix
Related Publications	xxi
Obtaining Documentation	xxi
Cisco.com	xxi
Documentation DVD	xxi
Ordering Documentation	xxii
Documentation Feedback	xxii
Cisco Product Security Overview	xxii
Reporting Security Problems in Cisco Products	xxiii
Obtaining Technical Assistance	xxiii
Cisco Technical Support Website	xxiii
Submitting a Service Request	xxiv
Definitions of Service Request Severity	xxiv
Obtaining Additional Publications and Information	xxv

CHAPTER 1

Overview	1-1
Features	1-1
Features Introduced in This Release	1-1
Existing Features	1-2
Management Options	1-3
Network Configuration Examples	1-3
Point-to-Point Bridging	1-4
Point-to-Multipoint Bridging	1-4
Redundant Bridging	1-5
Access Point Mode	1-5
Workgroup Bridge Mode	1-6
Troubleshooting	1-6

CHAPTER 2**Configuring the Access Point/Bridge for the First Time 2-1**

- Before You Start 2-2
 - Default IP Address and Role in Radio Network Behavior 2-2
- Obtaining and Assigning an IP Address 2-2
- Using the Console Port to Access the CLI 2-3
- Assigning an IP Address Using the CLI 2-4
- Connecting to the Access Point/Bridge Locally 2-4
- Assigning Basic Settings 2-5
 - Default Settings on the Express Setup Page 2-9
- Protecting Your Wireless LAN 2-10
- Configuring Basic Security Settings 2-10
 - Understanding Express Security Settings 2-11
 - Using VLANs 2-11
 - Express Security Types 2-11
 - Express Security Limitations 2-12
 - Using the Express Security Page 2-13
 - CLI Configuration Examples 2-13
- Using the IP Setup Utility 2-17
 - Obtaining and Installing IPSU 2-17
 - Using IPSU to Find the Access Point/Bridge's IP Address 2-18
- Using a Telnet Session to Access the CLI 2-19
- Resetting the Access Point/Bridge to Default Settings 2-19
 - Using the Web-Browser Interface 2-19
 - Using the CLI 2-20

CHAPTER 3**Using the Web-Browser Interface 3-1**

- Using the Web-Browser Interface for the First Time 3-2
- Using the Management Pages in the Web-Browser Interface 3-2
 - Using Action Buttons 3-3
 - Character Restrictions in Entry Fields 3-4
- Enabling HTTPS for Secure Browsing 3-4
 - CLI Configuration Example 3-11
 - Deleting an HTTPS Certificate 3-11
- Using Online Help 3-12
 - Changing the Location of Help Files 3-12
- Disabling the Web-Browser Interface 3-14

CHAPTER 4**Using the Command-Line Interface 4-1**

- IOS Command Modes 4-2
- Getting Help 4-3
- Abbreviating Commands 4-3
- Using no and default Forms of Commands 4-3
- Understanding CLI Messages 4-4
- Using Command History 4-4
 - Changing the Command History Buffer Size 4-4
 - Recalling Commands 4-5
 - Disabling the Command History Feature 4-5
- Using Editing Features 4-5
 - Enabling and Disabling Editing Features 4-6
 - Editing Commands Through Keystrokes 4-6
 - Editing Command Lines that Wrap 4-7
- Searching and Filtering Output of show and more Commands 4-8
- Accessing the CLI 4-8
 - Opening the CLI with Telnet 4-8
 - Opening the CLI with Secure Shell 4-9
 - Opening the CLI Using the Console Port 4-9

CHAPTER 5**Administering the Access Point/Bridge 5-1**

- Preventing Unauthorized Access to Your Access Point/Bridge 5-2
- Protecting Access to Privileged EXEC Commands 5-2
 - Default Password and Privilege Level Configuration 5-3
 - Setting or Changing a Static Enable Password 5-3
 - Protecting Enable and Enable Secret Passwords with Encryption 5-4
 - Configuring Username and Password Pairs 5-6
 - Configuring Multiple Privilege Levels 5-6
 - Setting the Privilege Level for a Command 5-7
 - Logging Into and Exiting a Privilege Level 5-8
- Controlling Access Point/Bridge Access with RADIUS 5-8
 - Default RADIUS Configuration 5-8
 - Configuring RADIUS Login Authentication 5-9
 - Defining AAA Server Groups 5-10
 - Configuring RADIUS Authorization for User Privileged Access and Network Services 5-12
 - Displaying the RADIUS Configuration 5-13
- Controlling Access Point/Bridge Access with TACACS+ 5-13
 - Default TACACS+ Configuration 5-14

Configuring TACACS+ Login Authentication	5-14
Configuring TACACS+ Authorization for Privileged EXEC Access and Network Services	5-15
Displaying the TACACS+ Configuration	5-16
Configuring Ethernet Speed and Duplex Settings	5-16
Configuring the Access Point/Bridge for Local Authentication and Authorization	5-17
Configuring the Authentication Cache and Profile	5-18
Configuring the Access Point/Bridge to Provide DHCP Service	5-21
Setting up the DHCP Server	5-21
Monitoring and Maintaining the DHCP Server Access Point	5-22
Show Commands	5-22
Clear Commands	5-23
Debug Command	5-23
Configuring the Access Point for Secure Shell	5-23
Understanding SSH	5-24
Configuring SSH	5-24
Configuring Client ARP Caching	5-24
Understanding Client ARP Caching	5-24
Optional ARP Caching	5-25
Configuring ARP Caching	5-25
Managing the System Time and Date	5-26
Understanding the System Clock	5-26
Understanding Network Time Protocol	5-26
Configuring NTP	5-28
Default NTP Configuration	5-28
Configuring NTP Authentication	5-28
Configuring NTP Associations	5-30
Configuring NTP Broadcast Service	5-31
Configuring NTP Access Restrictions	5-32
Configuring the Source IP Address for NTP Packets	5-34
Displaying the NTP Configuration	5-35
Configuring Time and Date Manually	5-35
Setting the System Clock	5-35
Displaying the Time and Date Configuration	5-36
Configuring the Time Zone	5-36
Configuring Summer Time (Daylight Saving Time)	5-37
Configuring a System Name and Prompt	5-38
Default System Name and Prompt Configuration	5-39
Configuring a System Name	5-39
Understanding DNS	5-39

Default DNS Configuration	5-40
Setting Up DNS	5-40
Displaying the DNS Configuration	5-41
Creating a Banner	5-41
Default Banner Configuration	5-41
Configuring a Message-of-the-Day Login Banner	5-41
Configuring a Login Banner	5-42

CHAPTER 6
Configuring Radio Settings 6-1

Enabling the Radio Interface	6-2
Configuring the Role in Radio Network	6-2
Configuring Radio Data Rates	6-5
Configuring Radio Transmit Power	6-7
Limiting the Power Level for Associated Client Devices	6-8
Configuring Radio Channel Settings	6-9
Configuring LBS on Access Points	6-10
Enabling and Disabling World Mode	6-11
Disabling and Enabling Short Radio Preambles	6-12
Configuring Transmit and Receive Antennas	6-13
Aironet Extensions	6-14
Configuring the Ethernet Encapsulation Transformation Method	6-15
Enabling and Disabling Concatenation	6-15
Configuring the Radio Distance Setting	6-16
Enabling and Disabling Reliable Multicast to Workgroup Bridges	6-16
Enabling and Disabling Public Secure Packet Forwarding	6-17
Configuring Protected Ports	6-18
Enabling Short Slot Time	6-19
Configuring the Beacon Period and the DTIM	6-19
Configure RTS Threshold and Retries	6-19
Configuring the Maximum Data Retries	6-20
Configuring the Fragmentation Threshold	6-21
Setting the Root Parent Timeout Value	6-21
Configuring the Root Parent MAC	6-22
Performing a Carrier Busy Test	6-22

CHAPTER 7
Configuring Multiple SSIDs 7-1

Understanding Multiple SSIDs	7-2

Effect of Software Versions on SSIDs	7-2
Configuring Multiple SSIDs	7-4
Default SSID Configuration	7-4
Creating an SSID Globally	7-4
Viewing SSIDs Configured Globally	7-6
Using Spaces in SSIDs	7-6
Using a RADIUS Server to Restrict SSIDs	7-6
Configuring Multiple Basic SSIDs	7-7
Requirements for Configuring Multiple BSSIDs	7-7
Guidelines for Using Multiple BSSIDs	7-8
Configuring Multiple BSSIDs	7-8
CLI Configuration Example	7-10
Displaying Configured BSSIDs	7-10
Assigning IP Redirection for an SSID	7-10
Guidelines for Using IP Redirection	7-11
Configuring IP Redirection	7-11
Including an SSID in an SSID IE	7-12

CHAPTER 8

Configuring Spanning Tree Protocol 8-1

Understanding Spanning Tree Protocol	8-2
STP Overview	8-2
350 Series Bridge Interoperability	8-3
Access Point/Bridge Protocol Data Units	8-3
Election of the Spanning-Tree Root	8-4
Spanning-Tree Timers	8-5
Creating the Spanning-Tree Topology	8-5
Spanning-Tree Interface States	8-6
Blocking State	8-7
Listening State	8-7
Learning State	8-8
Forwarding State	8-8
Disabled State	8-8
Configuring STP Features	8-8
Default STP Configuration	8-9
Configuring STP Settings	8-9
STP Configuration Examples	8-10
Root Bridge Without VLANs	8-10
Non-Root Bridge Without VLANs	8-11
Root Bridge with VLANs	8-12

Non-Root Bridge with VLANs	8-13
Displaying Spanning-Tree Status	8-14

CHAPTER 9

Configuring Cipher Suites and WEP	9-1
Understanding Cipher Suites and WEP	9-2
Configuring Cipher Suites and WEP	9-3
Creating WEP Keys	9-3
WEP Key Restrictions	9-4
Example WEP Key Setup	9-5
Enabling Cipher Suites and WEP	9-6
Matching Cipher Suites with WPA and CCKM	9-7
Enabling and Disabling Broadcast Key Rotation	9-7

CHAPTER 10

Configuring Authentication Types	10-1
Understanding Authentication Types	10-2
Open Authentication to the Access Point/Bridge	10-2
Shared Key Authentication to the Access Point/Bridge	10-3
EAP Authentication to the Network	10-4
MAC Address Authentication to the Network	10-5
Combining MAC-Based, EAP, and Open Authentication	10-6
Using CCKM for Authenticated Clients	10-6
Using WPA Key Management	10-7
Software and Firmware Requirements for WPA and WPA-TKIP	10-9
Configuring Authentication Types	10-9
Assigning Authentication Types to an SSID	10-10
Configuring WPA Migration Mode	10-12
Configuring the Root Access Point/Bridge to Interact with the WDS Device	10-13
Configuring Additional WPA Settings	10-13
Configuring Authentication Holdoffs, Timeouts, and Intervals	10-14
Matching Authentication Types on Root and Non-Root Access Point/Bridges	10-15

CHAPTER 11

Configuring WDS, Fast Secure Roaming, Radio Management, and Wireless Intrusion Detection Services	11-1
Understanding WDS	11-2
Role of the WDS Device	11-2
Role of Access Points Using the WDS Device	11-3
Understanding Fast Secure Roaming	11-3
Understanding Radio Management	11-4

Understanding Layer 3 Mobility	11-4
Understanding Wireless Intrusion Detection Services	11-6
Configuring WDS	11-6
Guidelines for WDS	11-7
Requirements for WDS	11-7
Configuration Overview	11-7
Configuring Access Point/Bridges as Potential WDS Devices	11-8
CLI Configuration Example	11-12
Configuring Access Points to use the WDS Device	11-13
CLI Configuration Example	11-14
Configuring the Authentication Server to Support WDS	11-14
Viewing WDS Information	11-20
Using Debug Messages	11-21
Configuring Fast Secure Roaming	11-21
Requirements for Fast Secure Roaming	11-21
Configuring Access Points to Support Fast Secure Roaming	11-22
CLI Configuration Example	11-24
Configuring Radio Management	11-25
CLI Configuration Example	11-26
Configuring Access Points to Participate in WIDS	11-27
Configuring the Access Point for Scanner Mode	11-27
Configuring the Access Point for Monitor Mode	11-27
Displaying Monitor Mode Statistics	11-28
Configuring Monitor Mode Limits	11-28
Configuring an Authentication Failure Limit	11-28

CHAPTER 12

Configuring RADIUS and TACACS+ Servers 12-1

Configuring and Enabling RADIUS	12-2
Understanding RADIUS	12-2
RADIUS Operation	12-3
Configuring RADIUS	12-4
Default RADIUS Configuration	12-4
Identifying the RADIUS Server Host	12-5
Configuring RADIUS Login Authentication	12-7
Defining AAA Server Groups	12-9
Configuring RADIUS Authorization for User Privileged Access and Network Services	12-11
Starting RADIUS Accounting	12-12
Selecting the CSID Format	12-13
Configuring Settings for All RADIUS Servers	12-13

Configuring the Access Point/Bridge to Use Vendor-Specific RADIUS Attributes	12-14
Configuring the Access Point/Bridge for Vendor-Proprietary RADIUS Server Communication	12-15
Configuring WISPr RADIUS Attributes	12-16
Displaying the RADIUS Configuration	12-17
RADIUS Attributes Sent by the Access Point/Bridge	12-18
Configuring and Enabling TACACS+	12-21
Understanding TACACS+	12-21
TACACS+ Operation	12-22
Configuring TACACS+	12-22
Default TACACS+ Configuration	12-23
Identifying the TACACS+ Server Host and Setting the Authentication Key	12-23
Configuring TACACS+ Login Authentication	12-24
Configuring TACACS+ Authorization for Privileged EXEC Access and Network Services	12-25
Starting TACACS+ Accounting	12-26
Displaying the TACACS+ Configuration	12-27

CHAPTER 13

Configuring VLANs 13-1

Understanding VLANs	13-2
Related Documents	13-3
Incorporating Wireless Access Point/Bridges into VLANs	13-4
Configuring VLANs	13-4
Configuring a VLAN	13-4
Viewing VLANs Configured on the Access Point/Bridge	13-7
Assigning Names to VLANs	13-7
Guidelines for Using VLAN Names	13-7
Creating a VLAN Name	13-8
Using a RADIUS Server to Assign Users to VLANs	13-8
Viewing VLANs Configured on the Access Point/Bridge	13-9
VLAN Configuration Example	13-9

CHAPTER 14

Configuring QoS 14-1

Understanding QoS for Wireless LANs	14-2
QoS for Wireless LANs Versus QoS on Wired LANs	14-2
Impact of QoS on a Wireless LAN	14-2
Precedence of QoS Settings	14-3
Using Wi-Fi Multimedia Mode	14-4
Configuring QoS	14-5
Configuration Guidelines	14-5

Configuring QoS Using the Web-Browser Interface	14-5
Adjusting Radio Access Category Definitions	14-9
Disabling IGMP Snooping Helper	14-11
Disabling AVVID Priority Mapping	14-11
CW-min and CW-max Settings for Point-to-Point and Point-to-Multipoint Bridge Links	14-11
QoS Configuration Examples	14-12
Giving Priority to Voice Traffic	14-12
Giving Priority to Video Traffic	14-13

CHAPTER 15

Configuring Filters 15-1

Understanding Filters	15-2
Configuring Filters Using the CLI	15-2
Configuring Filters Using the Web-Browser Interface	15-2
Configuring and Enabling MAC Address Filters	15-3
Creating a MAC Address Filter	15-4
Using MAC Address ACLs to Block or Allow Client Association to the Access Point	15-5
Configuring and Enabling IP Filters	15-7
Creating an IP Filter	15-8
Configuring and Enabling Ethertype Filters	15-10
Creating an Ethertype Filter	15-11

CHAPTER 16

Configuring CDP 16-1

Understanding CDP	16-2
Configuring CDP	16-2
Default CDP Configuration	16-2
Configuring the CDP Characteristics	16-3
Disabling and Enabling CDP	16-3
Disabling and Enabling CDP on an Interface	16-4
Monitoring and Maintaining CDP	16-5

CHAPTER 17

Configuring SNMP 17-1

Understanding SNMP	17-2
SNMP Versions	17-2
SNMP Manager Functions	17-3
SNMP Agent Functions	17-3
SNMP Community Strings	17-4
Using SNMP to Access MIB Variables	17-4
Configuring SNMP	17-5

Default SNMP Configuration	17-5
Enabling the SNMP Agent	17-5
Configuring Community Strings	17-5
Configuring Trap Managers and Enabling Traps	17-7
Setting the Agent Contact and Location Information	17-10
Using the snmp-server view Command	17-10
SNMP Examples	17-10
Displaying SNMP Status	17-11

CHAPTER 18

Managing Firmware and Configurations 18-1

Working with the Flash File System	18-2
Displaying Available File Systems	18-2
Setting the Default File System	18-3
Displaying Information About Files on a File System	18-3
Changing Directories and Displaying the Working Directory	18-4
Creating and Removing Directories	18-4
Copying Files	18-5
Deleting Files	18-5
Creating, Displaying, and Extracting tar Files	18-6
Creating a tar File	18-6
Displaying the Contents of a tar File	18-7
Extracting a tar File	18-7
Displaying the Contents of a File	18-8
Working with Configuration Files	18-8
Guidelines for Creating and Using Configuration Files	18-9
Configuration File Types and Location	18-10
Creating a Configuration File by Using a Text Editor	18-10
Copying Configuration Files by Using TFTP	18-10
Preparing to Download or Upload a Configuration File by Using TFTP	18-10
Downloading the Configuration File by Using TFTP	18-11
Uploading the Configuration File by Using TFTP	18-12
Copying Configuration Files by Using FTP	18-12
Preparing to Download or Upload a Configuration File by Using FTP	18-13
Downloading a Configuration File by Using FTP	18-13
Uploading a Configuration File by Using FTP	18-14
Copying Configuration Files by Using RCP	18-15
Preparing to Download or Upload a Configuration File by Using RCP	18-16
Downloading a Configuration File by Using RCP	18-17
Uploading a Configuration File by Using RCP	18-18

Clearing Configuration Information	18-18
Deleting a Stored Configuration File	18-18
Working with Software Images	18-19
Image Location on the Access Point/Bridge	18-19
tar File Format of Images on a Server or Cisco.com	18-20
Copying Image Files by Using TFTP	18-20
Preparing to Download or Upload an Image File by Using TFTP	18-20
Downloading an Image File by Using TFTP	18-21
Uploading an Image File by Using TFTP	18-23
Copying Image Files by Using FTP	18-23
Preparing to Download or Upload an Image File by Using FTP	18-24
Downloading an Image File by Using FTP	18-25
Uploading an Image File by Using FTP	18-27
Copying Image Files by Using RCP	18-28
Preparing to Download or Upload an Image File by Using RCP	18-28
Downloading an Image File by Using RCP	18-30
Uploading an Image File by Using RCP	18-32
Reloading the Image Using the Web Browser Interface	18-33
Browser HTTP Interface	18-33
Browser TFTP Interface	18-33

CHAPTER 19

Configuring System Message Logging	19-1
Understanding System Message Logging	19-2
Configuring System Message Logging	19-2
System Log Message Format	19-2
Default System Message Logging Configuration	19-3
Disabling and Enabling Message Logging	19-4
Setting the Message Display Destination Device	19-5
Enabling and Disabling Timestamps on Log Messages	19-6
Enabling and Disabling Sequence Numbers in Log Messages	19-6
Defining the Message Severity Level	19-7
Limiting Syslog Messages Sent to the History Table and to SNMP	19-8
Setting a Logging Rate Limit	19-9
Configuring UNIX Syslog Servers	19-10
Logging Messages to a UNIX Syslog Daemon	19-10
Configuring the UNIX System Logging Facility	19-10
Displaying the Logging Configuration	19-12

CHAPTER 20**Configuring Repeater and Standby Access Points and Workgroup Bridge Mode 20-1**

- Understanding Repeater Access Points 20-2
- Configuring a Repeater Access Point 20-3
 - Default Configuration 20-3
 - Guidelines for Repeaters 20-3
 - Setting Up a Repeater 20-4
 - Verifying Repeater Operation 20-5
 - Setting Up a Repeater As a LEAP Client 20-5
 - Setting Up a Repeater As a WPA Client 20-6
- Understanding Hot Standby 20-7
- Configuring a Hot Standby Access Point 20-7
 - Verifying Standby Operation 20-10
- Understanding Workgroup Bridge Mode 20-11
 - Treating Workgroup Bridges as Infrastructure Devices or as Client Devices 20-12
 - Configuring a Workgroup Bridge for Roaming 20-13
 - Configuring a Client VLAN 20-13
- Configuring Workgroup Bridge Mode 20-13

CHAPTER 21**Troubleshooting 21-1**

- Checking the LEDs 21-2
 - Normal Mode LED Indications 21-2
- Power Injector 21-4
- Checking Power 21-5
- Checking Basic Configuration Settings 21-5
 - SSID 21-5
 - WEP Keys 21-6
 - Security Settings 21-6
- Antenna Alignment 21-6
- Resetting the Access Point/Bridge to the Default Configuration 21-6
 - Using the Web-Browser Interface 21-7
 - Using the CLI 21-7
 - Corrupt IOS Configuration or Lost Password Procedure 21-8
- Reloading the Access Point/Bridge Image 21-9
 - Web-Browser Interface 21-9
 - Browser HTTP Interface 21-9
 - Browser TFTP Interface 21-10
 - Using the CLI 21-10
 - Obtaining the Access Point/Bridge Image File 21-12

Obtaining the TFTP Server Software 21-13

APPENDIX A

Protocol Filters B-1

APPENDIX B

Supported MIBs C-1

MIB List C-1

Using FTP to Access the MIB Files C-2

APPENDIX C

Error and Event Messages D-1

Conventions D-1

Software Auto Upgrade Messages D-2

Association Management Messages D-3

Unzip Messages D-4

802.11 Subsystem Messages D-5

Inter-Access Point Protocol Messages D-14

Local Authenticator Messages D-14

WDS Messages D-15

Mini IOS Messages D-16

GLOSSARY

INDEX



Preface

Audience

This guide is for the networking professional who installs and manages Cisco Aironet 1300 Series Outdoor Access Point/Bridge. To use this guide, you should have experience working with the Cisco IOS and be familiar with the concepts and terminology of wireless local area networks.

Purpose

This guide provides the information you need to install and configure your access point/bridge. This guide provides procedures for using the IOS commands that have been created or changed for use with the access point/bridge. It does not provide detailed information about these commands. For detailed information about these commands, refer to the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges* for this release. For information about the standard IOS Release 12.3 commands, refer to the IOS documentation set available from the Cisco.com home page. Click **Technical Documentation** in the Quick Links section.

This guide also includes an overview of the access point/bridge web-based interface, which contains all the functionality of the command-line interface (CLI). This guide does not provide field-level descriptions of the web-based windows nor does it provide the procedures for configuring the access point/bridge from the web-based interface. For all window descriptions and procedures, refer to the access point/bridge online help, which is available from the Help buttons on the web-based interface pages.

Organization

This guide is organized into these chapters:

[Chapter 1, “Overview,”](#) lists the software and hardware features of the access point/bridge and describes the access point/bridge’s role in your network.

[Chapter 2, “Configuring the Access Point/Bridge for the First Time,”](#) describes how to configure basic settings on a new access point/bridge.

[Chapter 3, “Using the Web-Browser Interface,”](#) describes how to use the web-browser interface to configure the access point/bridge.

[Chapter 4, “Using the Command-Line Interface,”](#) describes how to use the command-line interface (CLI) to configure the access point/bridge.

[Chapter 5, “Administering the Access Point/Bridge,”](#) describes how to perform one-time operations to administer your access point/bridge, such as preventing unauthorized access to the access point/bridge, setting the system date and time, and setting the system name and prompt.

[Chapter 6, “Configuring Radio Settings,”](#) describes how to configure settings for the access point/bridge radio such as the role in the radio network, data rates, transmit power, channel settings, and others.

[Chapter 7, “Configuring Multiple SSIDs,”](#) describes how to configure and manage multiple service set identifiers (SSIDs) on your access point/bridge. You can configure up to 16 SSIDs on your access point/bridge and assign different configuration settings to each SSID.

[Chapter 8, “Configuring Spanning Tree Protocol,”](#) describes how to configure Spanning Tree Protocol (STP) on your access point/bridge. STP prevents bridge loops in your network.

[Chapter 9, “Configuring Cipher Suites and WEP,”](#) describes how to configure the cipher suites required to use authenticated key management, Wired Equivalent Privacy (WEP), and WEP features including MIC, CMIC, TKIP, CKIP, and broadcast key rotation.

[Chapter 10, “Configuring Authentication Types,”](#) describes how to configure authentication types on the access point/bridge. Client devices use these authentication methods to join your network.

[Chapter 11, “Configuring WDS, Fast Secure Roaming, Radio Management, and Wireless Intrusion Detection Services,”](#) describes Wireless Domain Services (WDS), fast secure roaming, and radio management features. The chapter also provides instructions for configuring the access point/bridge to register with a WDS access point.

[Chapter 12, “Configuring RADIUS and TACACS+ Servers,”](#) describes how to enable and configure the Remote Authentication Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+), which provide detailed accounting information and flexible administrative control over authentication and authorization processes.

[Chapter 13, “Configuring VLANs,”](#) describes how to configure your access point/bridge to interoperate with the VLANs set up on your wired LAN.

[Chapter 14, “Configuring QoS,”](#) describes how to configure quality of service (QoS) on your access point/bridge. With this feature, you can provide preferential treatment to certain traffic at the expense of others.

[Chapter 15, “Configuring Filters,”](#) describes how to configure and manage MAC address, IP, and Ethertype filters on the access point/bridge using the web-browser interface.

[Chapter 16, “Configuring CDP,”](#) describes how to configure Cisco Discovery Protocol (CDP) on your access point/bridge. CDP is a device-discovery protocol that runs on all Cisco network equipment.

[Chapter 17, “Configuring SNMP,”](#) describes how to configure the Simple Network Management Protocol (SNMP) on your access point/bridge.

[Chapter 18, “Managing Firmware and Configurations,”](#) describes how to manipulate the Flash file system, how to copy configuration files, and how to archive (upload and download) software images.

[Chapter 19, “Configuring System Message Logging,”](#) describes how to configure system message logging on your access point/bridge.

[Chapter 20, “Configuring Repeater and Standby Access Points and Workgroup Bridge Mode,”](#) describes how to configure the access point/bridge as a repeater access point or workgroup bridge.

[Chapter 21, “Troubleshooting,”](#) provides troubleshooting procedures for basic problems with the access point/bridge.

[Appendix A, “Protocol Filters,”](#) lists some of the protocols that you can filter on the access point/bridge.

[Appendix B, “MIB List,”](#) lists the Simple Network Management Protocol (SNMP) Management Information Bases (MIBs) that the access point/bridge supports for this software release.

Appendix C, “Error and Event Messages,” lists the CLI error and event messages and provides an explanation and recommended action for each message.

Conventions

This publication uses these conventions to convey instructions and information:

Command descriptions use these conventions:

- Commands and keywords are in boldface text.
- Arguments for which you supply values are in italic.
- Square brackets ([]) mean optional elements.
- Braces ({ }) group required choices, and vertical bars (|) separate the alternative elements.
- Braces and vertical bars within square brackets ([{ | }]) mean a required choice within an optional element.

Interactive examples use these conventions:

- Terminal sessions and system displays are in screen font.
- Information you enter is in **boldface screen** font.
- Non printing characters, such as passwords or tabs, are in angle brackets (< >).

Notes, cautions, and timesavers use these conventions and symbols:



Tip

Means the following will help you solve a problem. The tips information might not be troubleshooting or even an action, but could be useful information.



Note

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



Caution

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



Warning

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. (To see translations of the warnings that appear in this publication, refer to the appendix “Translated Safety Warnings.”)

Waarschuwing

Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van standaard maatregelen om ongelukken te voorkomen. (Voor vertalingen van de waarschuwingen die in deze publicatie verschijnen, kunt u het aanhangsel “Translated Safety Warnings” (Vertalingen van veiligheidsvoorschriften) raadplegen.)

Varoitus	Tämä varoitusmerkki merkitsee vaaraa. Olet tilanteessa, joka voi johtaa ruumiinvammaan. Ennen kuin työskentelet minkään laitteiston parissa, ota selvää sähkökytkentöihin liittyvistä vaaroista ja tavanomaisista onnettomuuksien ehkäisykeinoista. (Tässä julkaisussa esiintyvien varoitusten käännökset löydät liitteestä "Translated Safety Warnings" (käännetyt turvallisuutta koskevat varoitukset).)
Attention	Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant entraîner des blessures. Avant d'accéder à cet équipement, soyez conscient des dangers posés par les circuits électriques et familiarisez-vous avec les procédures courantes de prévention des accidents. Pour obtenir les traductions des mises en garde figurant dans cette publication, veuillez consulter l'annexe intitulée « Translated Safety Warnings » (Traduction des avis de sécurité).
Warnung	Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu einer Körperverletzung führen könnte. Bevor Sie mit der Arbeit an irgendeinem Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidung von Unfällen bewußt. (Übersetzungen der in dieser Veröffentlichung enthaltenen Warnhinweise finden Sie im Anhang mit dem Titel "Translated Safety Warnings" (Übersetzung der Warnhinweise).)
Avvertenza	Questo simbolo di avvertenza indica un pericolo. Si è in una situazione che può causare infortuni. Prima di lavorare su qualsiasi apparecchiatura, occorre conoscere i pericoli relativi ai circuiti elettrici ed essere al corrente delle pratiche standard per la prevenzione di incidenti. La traduzione delle avvertenze riportate in questa pubblicazione si trova nell'appendice, "Translated Safety Warnings" (Traduzione delle avvertenze di sicurezza).
Advarsel	Dette varselsymbolet betyr fare. Du befinner deg i en situasjon som kan føre til personskade. Før du utfører arbeid på utstyr, må du være oppmerksom på de faremomentene som elektriske kretser innebærer, samt gjøre deg kjent med vanlig praksis når det gjelder å unngå ulykker. (Hvis du vil se oversettelser av de advarslene som finnes i denne publikasjonen, kan du se i vedlegget "Translated Safety Warnings" [Oversatte sikkerhetsadvarsler].)
Aviso	Este símbolo de aviso indica perigo. Encontra-se numa situação que lhe poderá causar danos físicos. Antes de começar a trabalhar com qualquer equipamento, familiarize-se com os perigos relacionados com circuitos eléctricos, e com quaisquer práticas comuns que possam prevenir possíveis acidentes. (Para ver as traduções dos avisos que constam desta publicação, consulte o apêndice "Translated Safety Warnings" - "Traduções dos Avisos de Segurança").
¡Advertencia!	Este símbolo de aviso significa peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considerar los riesgos que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención de accidentes. (Para ver traducciones de las advertencias que aparecen en esta publicación, consultar el apéndice titulado "Translated Safety Warnings.")
Varning!	Denna varningssymbol signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanligt förfarande för att förebygga skador. (Se förklaringar av de varningar som förekommer i denna publikation i appendix "Translated Safety Warnings" [Översatta säkerhetsvarningar].)

Related Publications

These documents provide complete information about the access point/bridge:

- *Quick Start Guide Cisco Aironet 1300 Series Bridge*
- *Release Notes for 1300 Series Access Point/Bridges*
- *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*

Click this link to browse to the Cisco Aironet documentation home page:

<http://www.cisco.com/univercd/cc/td/doc/product/wireless/index.htm>

To browse to the 1300 series access point/bridge documentation, select **Products and Solutions > Products > Wireless > All Wireless Products > Cisco Aironet 1300 Series > Technical Documentation**.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

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

Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

Cisco Marketplace:

<http://www.cisco.com/go/marketplace/>

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:
<http://www.cisco.com/en/US/partner/ordering/>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

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

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

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com

**Tip**

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

<http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on>

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

**Note**

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID

or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

<http://www.cisco.com/ipj>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>



Overview

Cisco Aironet 1300 Series Outdoor Access Points/Bridges (hereafter called *access points/bridges*) provide campus building-to-building wireless connectivity. Operating in the 2.4-GHz ISM band and conforming to the 802.11g standard, the 1300 series access point/bridge delivers a 54-Mbps data rate. The access point/bridge communicates with any 802.11b or 802.11g clients when in the access point mode and other 1300 series access points/bridges when in the bridging mode.

The access point/bridge is a self-contained unit designed for outdoor installations but can also be used inside with a window mounting option. You can connect external antennas to the access point/bridge to attain various antenna gains and coverage patterns. The access point/bridge supports both point-to-point and point-to-multipoint configurations. Two point-to-point links (three links if 802.11b) can be stacked in order to increase data throughput or provide cold standby redundancy.

You can configure and monitor the access point/bridge using the command-line interface (CLI), the browser-based management system, or Simple Network Management Protocol (SNMP).

This chapter provides information on the following topics:

- [Existing Features, page 1-2](#)
- [Management Options, page 1-3](#)
- [Network Configuration Examples, page 1-3](#)
- [Troubleshooting, page 1-6](#)

Features

This section lists features supported on access pointWireless devices running Cisco IOS software.

Features Introduced in This Release

- AAA Authentication/Authorization Cache and Profile—This feature reduces the authentication load on RADIUS/TACACS servers caused when loading GUI pages by caching the authentication locally on the access point so only one authentication with the RADIUS/TACACS server is performed.



Note

The feature is supported only for administrative authentication on the access point. Other uses of this feature are not recommended and not supported.

- Secure Shell version 2 (SSHv2) support—SSH v2 is a standards-based protocol to provide secure Telnet capability for router configuration and administration.

Existing Features

Access point/bridges running Cisco IOS offer these software features:

- Antenna alignment assistance—Use this feature access an auto configuration and installation mode for quick deployment of point-to-point links without the need to configure the access point/bridge via Telnet, FTP, or Simple Network Management Protocol (SNMP). LEDs show signal strength information used in the installation and antenna alignment process.
- Automatic channel selection—This feature determines and selects the least congested channel to provide the least interference possible.
- Automatic rate scaling—This feature scales down the data rate to maintain connectivity at outlying distances.
- Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2)—Provides access control via per-user, per-session mutual authentication and data privacy via strong dynamic encryption.
- Enhanced security—Enable three advanced security features to protect against sophisticated attacks on your wireless network's WEP keys: Message Integrity Check (MIC), WEP key hashing, and broadcast WEP key rotation.
- Enhanced authentication services—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 Light Extensible Authentication Protocol (LEAP), Cisco's wireless authentication method, and receives and uses dynamic WEP keys.
- World mode—Use this feature to communicate the access point/bridge's regulatory setting information, including maximum transmit power and available channels, to world mode-enabled clients. Clients using world mode can be used in countries with different regulatory settings and automatically conform to local regulations.
- Multiple SSIDs—Create up to 16 SSIDs on the wireless device and assign any combination of these settings to each SSID:
 - Broadcast SSID mode for guests on your network
 - Client authentication methods
 - Maximum number of client associations
 - VLAN identifier
 - RADIUS accounting list identifier
 - A separate SSID for infrastructure devices such as repeaters and workgroup bridges
- QoS—Use this feature to support quality of service for prioritizing traffic from the Ethernet to the access point/bridge. The access point/bridge also supports the voice-prioritization schemes used by 802.11b wireless phones such as Spectralink's Netlink™ and Symbol's Netvision™.
- TACACS+ administrator authentication—Enable TACACS+ for server-based, detailed accounting information and flexible administrative control over authentication and authorization processes. It provides secure, centralized validation of administrators attempting to gain access to the wireless device.
- RADIUS Accounting—Enable accounting on the access point/bridge to send accounting data about wireless client devices to a RADIUS server on your network.

- TACACS+ administrator authentication—Enable TACACS+ for server-based, detailed accounting information and flexible administrative control over authentication and authorization processes. It provides secure, centralized validation of administrators attempting to gain access to your access point/bridge.
- Fast Secure Roaming—When configured as an access point the 1300 series allows authenticated client devices to roam securely from one access point to another without any perceptible delay during reassociation.
- Port Aggregation Protocol and Cisco Fast EtherChannel Technology—Bandwidth can be increased between bridged networks through the aggregation of multiple bridges at each site.
- Hot Standby—The access point/bridge supports failover to a standby device.
- Load balancing—The access point/bridge distributes user connections across available access points to optimize aggregate throughput.
- Link distance adjustment—Allows users to tune the Carrier Sense Multiple Access Collision Avoidance (CSMA/CA) parameters for a particular range to maximize performance.
- Wireless packet concatenation—Provides higher overall data throughput by concatenating smaller packets into larger ones.
- Wireless programmable clear-channel assessment—The access point/bridge can be configured to the particular background interference level found in your environment for reduced contention overhead with other wireless systems.
- CiscoWorks Wireless LAN Solution Engine (WLSE)—A component of Cisco Structured Wireless-Aware Network (SWAN), is an available management tool for the access point/bridge. The WLSE has an HTML-based management interface and uses SNMP and Secure Shell (SSH)/Secure Sockets Layer (SSL) for managing Cisco Aironet access points and bridges via a web browser.

Management Options

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

- The IOS command-line interface (CLI), which you use through a Telnet session. Most of the examples in this manual are taken from the CLI. [Chapter 4, “Using the Command-Line Interface,”](#) provides a detailed description of the CLI.
- A web-browser interface, which you use through a web browser. [Chapter 3, “Using the Web-Browser Interface,”](#) provides a detailed description of the web-browser interface.
- Simple Network Management Protocol (SNMP). [Chapter 17, “Configuring SNMP,”](#) explains how to configure your access point/bridge for SNMP management.

Network Configuration Examples

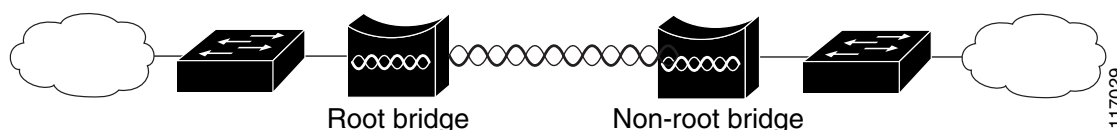
This section describes the access point/bridge’s role in common wireless bridging configurations: point-to-point, point-to-multipoint, redundant bridging, access point mode, and workgroup bridge mode. One bridge in any pair or group of bridges must be a root bridge, and the bridge or bridges associated to the root bridge must be set to non-root.

Point-to-Point Bridging

In a point-to-point configuration, a non-root bridge associates to a root bridge. In installation mode, the bridge listens for another 1300 series bridge. If it does not recognize another bridge, the bridge becomes a root bridge. If it recognizes another bridge, it becomes a non-root bridge associated to the bridge it recognizes. See [Chapter 2, “Configuring the Access Point/Bridge for the First Time,”](#) for instructions on initial bridge setup.

Figure 1-1 shows bridges in a point-to-point configuration.

Figure 1-1 *Point-to-Point Bridge Configuration*



Note

If your bridges connect one or more large, flat networks (a network containing more than 256 users on the same subnet) we recommend that you use a router to connect the bridge to the large, flat network.

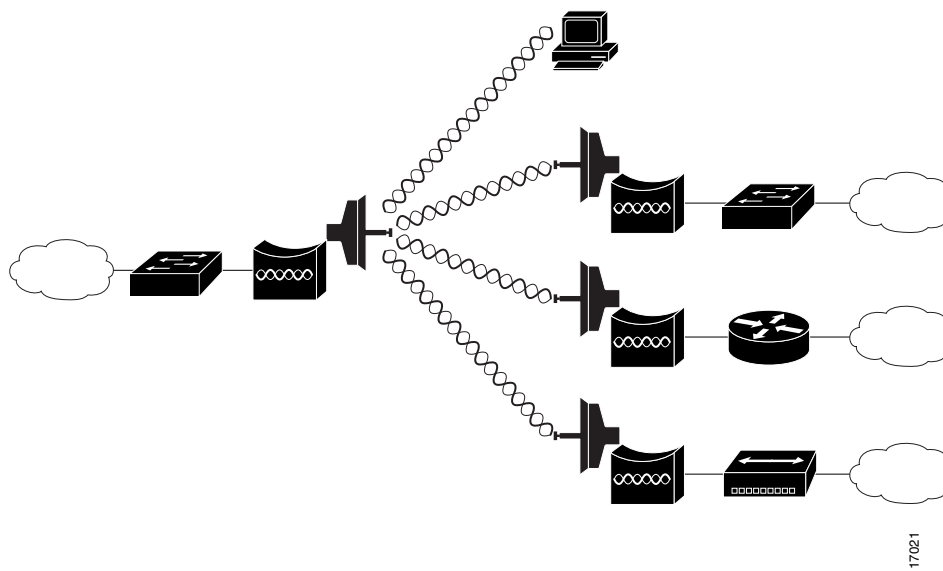
Point-to-Multipoint Bridging

In a point-to-multipoint configuration, two or more non-root bridges associate to a root bridge. Up to 17 non-root bridges can associate to a root bridge, but the non-root bridges must share the available bandwidth.

See [Chapter 2, “Configuring the Access Point/Bridge for the First Time,”](#) for instructions on initial bridge setup.

Figure 1-2 shows bridges in a point-to-multipoint configuration.

Figure 1-2 *Point-to-Multipoint Bridge Configuration*



**Note**

If your bridges connect one or more large, flat networks (a network containing more than 256 users on the same subnet) we recommend that you use a router to connect the bridge to the large, flat network.

Redundant Bridging

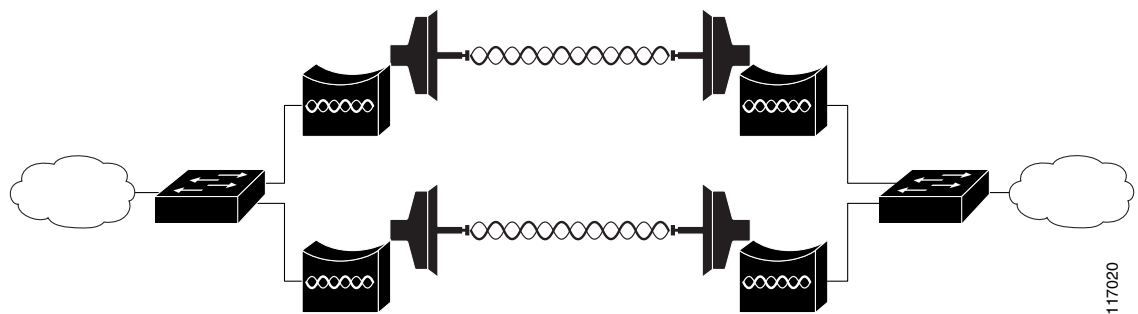
You can set up two pairs of bridges to add redundancy or load balancing to your bridge link. The bridges must use non-adjacent, non-overlapping radio channels to prevent interference, and they must use Spanning Tree Protocol (STP) to prevent bridge loops. See [Chapter 8, “Configuring Spanning Tree Protocol,”](#) for instructions on configuring STP.

**Note**

STP is disabled by default.

[Figure 1-3](#) shows two pairs of redundant bridges.

Figure 1-3 Redundant Bridge Configuration



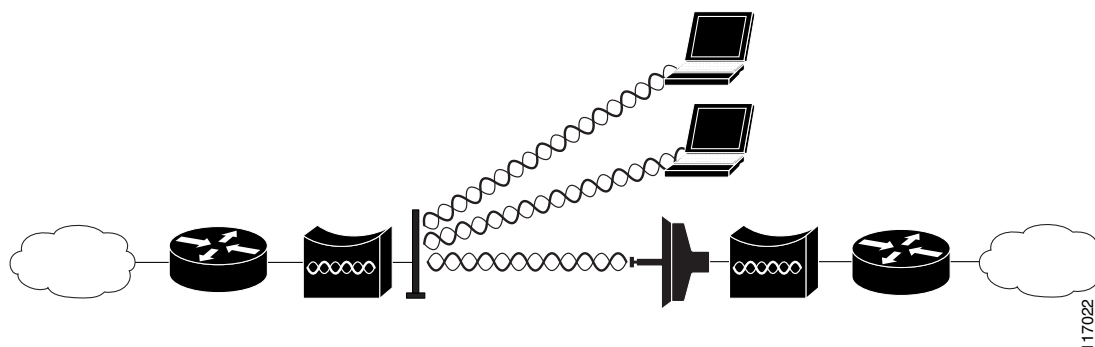
117020

Access Point Mode

You can configure the access point/bridge to function as an access point. In the access point mode, the access point/bridge emulates a Cisco Aironet 1100 Series Access Point. In the access point mode, the access point/bridge accepts associations from client devices. See [Chapter 20, “Configuring Repeater and Standby Access Points and Workgroup Bridge Mode,”](#) for instructions on configuring the access point/bridge as an access point.

[Figure 1-4](#) Shows a typical scenario where the access point/bridge functions as an access point.

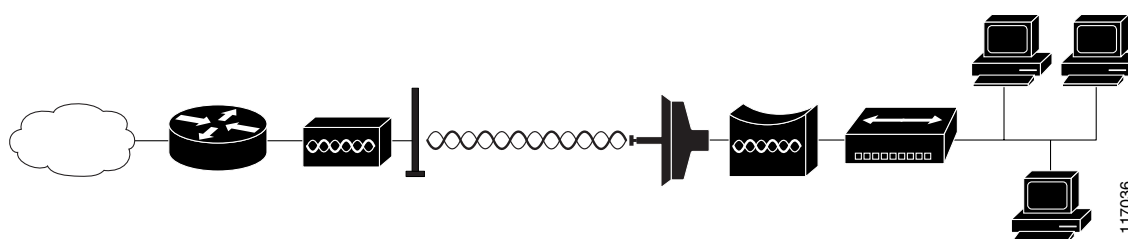
Figure 1-4 Access Point Mode



Workgroup Bridge Mode

You can configure the access point/bridge to function as a workgroup bridge. In the workgroup bridge mode, the access point/bridge emulates a Cisco Aironet 350 Series Workgroup Bridge; [Figure 1-5](#) shows a typical scenario where the access point/bridge functions as a workgroup bridge. See [Chapter 20, “Configuring Repeater and Standby Access Points and Workgroup Bridge Mode,”](#) for instructions on how to configure the access point/bridge as a workgroup bridge.

Figure 1-5 Workgroup Bridge Mode



Troubleshooting

For basic troubleshooting procedures, refer to the “Troubleshooting” chapter in the *Cisco Aironet 1300 Series Outdoor Access Point/Bridge Hardware Installation Guide*.

For the most up-to-date, detailed troubleshooting information, refer to the Cisco TAC website at <http://www.cisco.com/tac>. Click **Technology Support**, select **Wireless/Mobility** from the menu on the left, and click **Wireless LAN**.



Configuring the Access Point/Bridge for the First Time

This chapter describes how to configure basic settings on your access point/bridge for the first time. You can configure all the settings described in this chapter using the CLI, but it might be simplest to browse to the access point/bridge's web-browser interface to complete the initial configuration and then use the CLI to enter additional settings for a more detailed configuration.

This chapter contains these sections:

- [Before You Start, page 2-2](#)
- [Obtaining and Assigning an IP Address, page 2-2](#)
- [Assigning Basic Settings, page 2-5](#)
- [Configuring Basic Security Settings, page 2-10](#)
- [Using the IP Setup Utility, page 2-17](#)
- [Using a Telnet Session to Access the CLI, page 2-19](#)
- [Resetting the Access Point/Bridge to Default Settings, page 2-19](#)

Before You Start

For security reasons, the access point/bridge ships with no configuration and its radio disabled. You must configure the access point/bridge, which includes assigning at least one Service Set Identifier (SSID), which enables the access point/bridge's radio.

Before you install the access point/bridge, make sure you are using a computer connected to the same network as the access point/bridge, and obtain the following information from your network administrator:

- A host name for the access point/bridge
- An SSID
- If not connected to a DHCP server, a unique IP address for your access point/bridge (such as 172.17.255.115)
- If the access point/bridge is not on the same subnet as your PC, a default gateway address and subnet mask
- A Simple Network Management Protocol (SNMP) community name and the SNMP file attribute (if SNMP is in use)
- If you use IPSU to find the access point/bridge IP address, the MAC address from the product label on the access point/bridge (such as 00164625854c)

Default IP Address and Role in Radio Network Behavior

When you connect a 1300 series access point/bridge with a default configuration to your LAN, the access point/bridge attempts to get an IP address from the DHCP server. If no DHCP server is found, the access point/bridge continues to request a DHCP address. To eliminate this condition, you must connect to the access point/bridge using its console port. See the [“Using the Console Port to Access the CLI” section on page 2-3](#) for further information.

The access point/bridge assumes a radio network role of a root access point. To configure it as a bridge, you must manually place it in Install Mode in order to align the antennas and establish a link. In the Install Mode, one access point/bridge must be configured as a root bridge and the other a non-root bridge. To facilitate the configuration, an automatic option is available when the access point/bridge is in the install mode. After the wireless link is established and the bridge antennas are aligned, you take both access point/bridges out of Install Mode and place them on your LAN as root and non-root bridges.

Obtaining and Assigning an IP Address

To browse to the access point/bridge's Express Setup page, you must either obtain or assign the access point/bridge's IP address using one of the following methods:

- Assign a static IP address using the access point/bridge console port. For more information, see the [“Assigning an IP Address Using the CLI” section on page 2-4](#)
- Use a DHCP server (if available) to automatically assign an IP address. You can find out the DHCP-assigned IP address using one of the following methods:
 - Provide your organization's network administrator with your access point/bridge's Media Access Control (MAC) address. Your network administrator will query the DHCP server using the MAC address to identify the IP address. The access point/bridge's MAC address is on the label attached to the bottom of the access point/bridge.

- If a DHCP server is present, use the Cisco IP Setup Utility (IPSU) to identify an assigned IP address. You cannot assign an IP address using IPSU. IPSU runs on most Microsoft Windows operating systems: Windows 9x, 2000, Me, NT, and XP.

You can download IPSU from the Software Center on Cisco.com. Click this link to browse to the Software Center:

<http://www.cisco.com/cisco/software/navigator.html>

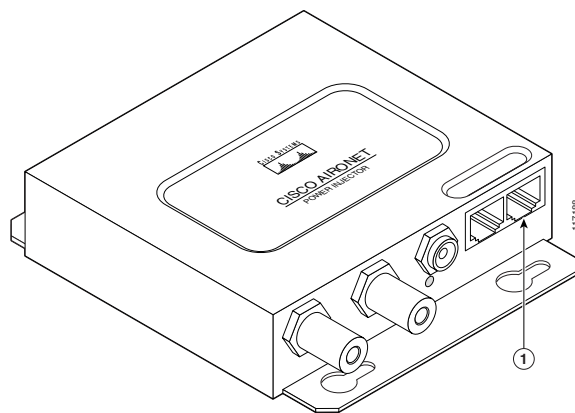
- If the unit is a non-root bridge, browse to the Associations page on the root bridge to which the non-root is associated. The non-root bridge's MAC address and IP address appear on the root bridge's Associations page.

Using the Console Port to Access the CLI

Follow these steps to access the CLI by connecting to the serial port:

- Step 1** Connect a nine-pin, female DB-9 to RJ-45 serial cable to the RJ-45 serial port on the power injector and to the COM port on your PC. [Figure 2-1](#) shows the power injector's serial port connector.

Figure 2-1 Serial Port Connector



1	Serial port connector (RJ-45 connector)



Note

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

- Step 2** Set up a terminal emulator to communicate with the access point/bridge. Use the following settings for the terminal emulator connection: 9600 baud, 8 data bits, no parity, 1 stop bit, and no flow control.
- Step 3** When the terminal emulator is activated, press **Enter**. An Enter Network Password window appears.
- Step 4** Enter your username in the User Name field. The default username is *Cisco*.
- Step 5** Enter the access point/bridge password in the Password field and press **Enter**. The default password is *Cisco*.

When the CLI activates, you can enter CLI commands to configure the access point/bridge.

Assigning an IP Address Using the CLI

When you connect the access point/bridge to the wired LAN, the access point/bridge links to the network using a bridge virtual interface (BVI) that it creates automatically. Instead of tracking separate IP addresses for the access point/bridge’s Ethernet and radio ports, the network uses the BVI.



Note The access point/bridge supports only one BVI. Configuring more than one BVI might cause errors in the access point/bridge’s ARP table.

When you assign an IP address to the access point/bridge using the CLI, you must assign the address to the BVI. Beginning in privileged EXEC mode, follow these steps to assign an IP address to the access point/bridge’s BVI and assign an IP address and subnet mask (address mask):

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface bvi1	Enter interface configuration mode for the BVI.
Step 3	ip address <i>address mask</i>	Assign an IP address and address mask to the BVI. Note If you are connected to the access point/bridge using a Telnet session, you lose your connection to the access point/bridge when you assign a new IP address to the BVI. If you need to continue configuring the bridge using Telnet, use the new IP address to open another Telnet session to the access point/bridge. Note If you do not assign an address mask, the address 255.255.255.224 is assigned automatically.
Step 4	end	Returns to privileged EXEC mode. Note You can also use Ctrl-Z to return to the privileged EXEC mode.
Step 5	show running-config	Verify your entry.
Step 6	copy running-config startup-config	(Optional) Save your entry in the configuration file.

When you have configured the access point/bridge IP address, you can use your Internet browser to access the unit’s graphical user interface (GUI).

Connecting to the Access Point/Bridge Locally

If you need to configure the access point/bridge locally (without connecting the access point/bridge to a wired LAN), you can connect a PC to the Ethernet port on the long-reach power injector using a Category 5 Ethernet cable. You can use a local connection to the power injector’s Ethernet port much as you would use a serial port connection.

**Note**

You do not need a special crossover cable to connect your PC to the power injector; you can use either a straight-through cable or a crossover cable.

Follow these steps to connect to the bridge locally:

Step 1 Make sure that the PC you intend to use is configured to obtain an IP address automatically, or manually assign it an IP address within the same subnet as the access point/bridge IP address. For example, if you assigned the access point/bridge an IP address of 10.0.0.1, assign the PC an IP address of 10.0.0.20.

Step 2 With the power cable disconnected from the power injector, connect your PC to the power injector using a Category 5 Ethernet cable. You can use either a crossover cable or a straight-through cable.

**Note**

Communication takes place between the power injector and the access point/bridge using Ethernet Port 0. Do not attempt to change any of the Ethernet Port 0 settings.

Step 3 Connect the power injector to the access point/bridge using dual coaxial cables.

Step 4 Connect the power injector power cable and power up the access point/bridge.

Step 5 Follow the steps in the [“Assigning Basic Settings” section on page 2-5](#). If you make a mistake and need to start over, follow the steps in the [“Resetting the Access Point/Bridge to Default Settings” section on page 2-19](#).

Step 6 After configuring the access point/bridge, remove the Ethernet cable from your PC and connect the power injector to your wired LAN.

**Note**

When you connect your PC to the access point/bridge or reconnect your PC to the wired LAN, you might need to release and renew the IP address on the PC. On most PCs, you can perform a release and renew by rebooting your PC or by entering **ipconfig /release** and **ipconfig /renew** commands in a command prompt window. Consult your PC operating instructions for detailed instructions.

Assigning Basic Settings

After you determine or assign the access point/bridge's IP address, you can browse to the access point/bridge's Express Setup page and perform an initial configuration:

Step 1 Open your Internet browser. The access point/bridge web-browser interface is fully compatible with these browsers: Microsoft Internet Explorer versions 5.0, 5.01, 5.5 and 6.0; and Netscape Navigator versions 4.79 and 7.0.

Step 2 Enter the access point/bridge's IP address in the browser address line and press **Enter**. An Enter Network Password screen appears.

Step 3 Enter the case-sensitive username *Cisco* and press **Tab** to advance to the Password field.

Step 4 Enter the case-sensitive password *Cisco* and press **Enter**. The Summary Status page appears. [Figure 2-2](#) shows the Summary Status page.

Figure 2-2 Summary Status Page

HOME
EXPRESS SET-UP
EXPRESS SECURITY
NETWORK MAP +
ASSOCIATION +
NETWORK INTERFACES +
SECURITY +
SERVICES +
WIRELESS SERVICES +
SYSTEM SOFTWARE +
EVENT LOG +

Hostname bridge

bridge uptime is 47 minutes

Home: Summary Status

Association

Clients: 0

Infrastructure clients: 0

Network Identity

IP Address

10.0.0.1

MAC Address

0005.9a3f.57f4

Network Interfaces

Interface	MAC Address	Transmission Rate
↑ FastEthernet	0005.9a3f.57f4	100Mb/s
↑ Radio0-802.11G	000e.8319.2800	54.0Mb/s

Event Log

Time	Severity	Description
Mar 1 00:01:40.876	◆ Notification	Line protocol on Interface Dot11Radio0, changed state to up
Mar 1 00:01:39.882	◆ Error	Interface Dot11Radio0, changed state to up
Mar 1 00:01:39.875	◆ Warning	Root selected
Mar 1 00:00:50.307	◆ Warning	Interface Dot11Radio0, cannot associate: No matching SSID
Mar 1 00:00:40.355	◆ Notification	Interface Dot11Radio0, changed state to reset
Mar 1 00:00:40.354	◆ Warning	Non-root - scanning for root
Mar 1 00:00:34.307	◆ Information	Interface Dot11Radio0, frequency 2447 selected
Mar 1 00:00:26.409	◆ Notification	Line protocol on Interface Dot11Radio0, changed state to down
Mar 1 00:00:26.375	◆ Notification	Line protocol on Interface BV11, changed state to up
Mar 1 00:00:25.448	◆ Notification	Interface Dot11Radio0, changed state to administratively down

Refresh

Step 5 Click **Express Setup**. The Express Setup screen appears. [Figure 2-3](#) shows the Express Setup page.

Figure 2-3 Express Setup Page

HOME | Hostname root | root uptime is 5 days, 22 hours, 47 minutes

EXPRESS SET-UP

EXPRESS SECURITY
NETWORK MAP +
ASSOCIATION +
NETWORK INTERFACES +
SECURITY +
SERVICES +
WIRELESS SERVICES +
SYSTEM SOFTWARE +
EVENT LOG +

Express Set-Up

Host Name:

MAC Address: 0012.016c.0240

Configuration Server Protocol: ☐ DHCP ☒ Static IP

IP Address:

IP Subnet Mask:

Default Gateway:

SNMP Community:

☒ Read-Only ☐ Read-Write

Radio0-802.11G

Role in Radio Network: ☒ Root ☐ Non-Root ☐ Install-Mode

☐ Non-Root with Clients

☐ Root AP ☐ Repeater AP

☐ Workgroup Bridge

Optimize Radio Network for: ☐ Throughput ☐ Range ☒ Default ☐ Custom

Aironet Extensions: ☒ Enable ☐ Disable

Apply Cancel

Step 6 Enter the configuration settings you obtained from your system administrator. The configurable settings include:

- **Host Name**—The host name, while not an essential setting, helps identify the access point/bridge on your network. The host name appears in the titles of the management system pages.

**Note**

You can enter up to 32 characters for the host name. However, when the wireless device identifies itself to client devices, it uses only the first 15 characters in the host name. If it is important for client users to distinguish between wireless devices, make sure a unique portion of the host name appears in the first 15 characters.

**Note**

When you change the host name, the wireless device resets the radios, causing associated client devices to disassociate and quickly reassociate.

- **Configuration Server Protocol**—Click on the button that matches the network's method of IP address assignment.
 - **DHCP**—IP addresses are automatically assigned by your network's DHCP server.
 - **Static IP**—The access point/bridge uses a static IP address that you enter in the IP address field.
- **IP Address**—Use this setting to assign or change the access point/bridge's IP address. If DHCP is enabled for your network, leave this field blank.

**Note**

If the access point/bridge's IP address changes while you are configuring the access point/bridge using the web-browser interface or a Telnet session over the wired LAN, you lose your connection to the access point/bridge. If you lose your connection, reconnect to the access point/bridge using its new IP address. Follow the steps in the [“Resetting the Access Point/Bridge to Default Settings”](#) section on page 2-19 if you need to start over.

- **IP Subnet Mask**—Enter the IP subnet mask provided by your network administrator so the IP address can be recognized on the LAN. If DHCP is enabled, leave this field blank.
- **Default Gateway**—Enter the default gateway IP address provided by your network administrator. If DHCP is enabled, leave this field blank.
- **SNMP Community**—If your network is using SNMP, enter the SNMP Community name provided by your network administrator and select the attributes of the SNMP data (also provided by your network administrator).
- **Role in Radio Network**—Click on the button that describes the role of the access point/bridge on your network.
 - **Access Point**—A root device; accepts associations from clients and bridges wireless traffic from the clients to the wireless LAN. This setting can be applied to any access point.
 - **Repeater**—A non-root device; accepts associations from clients and bridges wireless traffic from the clients to root access point connected to the wireless LAN. This setting can be applied to any access point.
 - **Root Bridge**—Establishes a link with a non-root bridge. In this mode, the device also accepts associations from clients.
 - **Non-Root Bridge**—In this mode, the device establishes a link with a root bridge.
 - **Install Mode**—Places the access point/bridge into installation mode so you can align and adjust a bridge link for optimum efficiency.
 - **Workgroup Bridge**—Emulates a Cisco Aironet 350 Series Workgroup Bridge. In the Workgroup bridge mode, the access point functions as a client device that associates with a Cisco Aironet access point or bridge.
 - **Scanner**—Performs as a network monitoring device. In the Scanner mode, the access point does not accept associations from clients. It continuously scans and reports wireless traffic it detects from other wireless devices on the wireless LAN. All access points can be configured as a scanner.

**Note**

The access point/bridge defaults to the Root AP mode. It must be manually set to the Install-Mode for use as a bridge. In bridge modes, one bridge in any pair or group of bridges must be set to root, and the bridge or bridges associated to the root bridge must be set to non-root.

- **Optimize Radio Network for**—Use this setting to select either preconfigured settings for the access point/bridge radio or customized settings for the access point/bridge radio. See the [“Configuring the Radio Distance Setting”](#) section on page 6-16 for more information on data rates and throughput.
 - **Throughput**—Maximizes the data volume handled by the access point/bridge but might reduce its range. When you select **Throughput**, the access point/bridge sets all data rates to **basic**.
 - **Range**—Maximizes the access point/bridge's range but might reduce throughput. When you select **Range**, the access point/bridge sets the 6-Mbps rate to **basic** and the other rates to **enabled**.

- **Default**—The access point/bridge retains default radio settings that are designed to provide good range and throughput for most access point/bridges.
- **Custom**—Takes you to the Network Interfaces: Radio-802.11G Settings page. The access point/bridge uses settings you enter on this page.
- **Aironet Extensions**—This setting is always enabled on 1300 series access point/bridges.

Step 7 Click **Apply** to save your settings. If you changed the IP address, you lose your connection to the access point/bridge. Browse to the new IP address to reconnect to the access point/bridge.

Your access point/bridge is now running but probably requires additional configuring to conform to your network's operational and security requirements.

Default Settings on the Express Setup Page

Table 2-1 lists the default settings for the settings on the Express Setup page.

Table 2-1 *Default Settings on the Express Setup Page*

Setting	Default
Host Name	ap
Configuration Server Protocol	DHCP
IP Address	Assigned by DHCP by default. See Default IP Address and Role in Radio Network Behavior, page 2-2 .
IP Subnet Mask	Assigned by DHCP by default; if DHCP is disabled, no IP subnet mask is assigned.
Default Gateway	Assigned by DHCP by default; if DHCP is disabled, no default gateway is assigned.
SNMP Community	defaultCommunity
Role in Radio Network	Root AP
Optimize Radio Network for	Default
Aironet Extensions	Enable

Protecting Your Wireless LAN

After you assign basic settings to your access point/bridge, you must configure security settings to prevent unauthorized access to your network. Because it is a radio device, the access point/bridge can communicate beyond the physical boundaries of your building. You can use Express Security page in the [Configuring Basic Security Settings](#) section to set basic security settings for your access point/bridge. Advanced security features can be found in the following chapters:

- A unique SSID that are not broadcast in the access point/bridge beacon (see [Chapter 7, “Configuring Multiple SSIDs”](#))
- WEP and WEP features (see [Chapter 9, “Configuring Cipher Suites and WEP”](#))
- Dynamic WEP and access point/bridge authentication (see [Chapter 10, “Configuring Authentication Types”](#))

Configuring Basic Security Settings

After you assign basic settings to your access point, you must configure security settings to prevent unauthorized access to your network. Because it is a radio device, the access point can communicate beyond the physical boundaries of your worksite.

Just as you use the Express Setup page to assign basic settings, you can use the Express Security page to create unique SSIDs and assign one of four security types to them. [Figure 2-4](#) shows the Express Security page.

Figure 2-4 Express Security Page

Hostname: bridge bridge uptime is 51 minutes

Express Security Set-Up

SSID Configuration

1. SSID ☐ Broadcast SSID in Beacon

2. VLAN

☒ No VLAN ☐ Enable VLAN ID: (1-4095) ☐ Native VLAN

3. Security

☒ No Security

☐ Static WEP Key

Key 1 128 bit

☐ EAP Authentication

RADIUS Server: (Hostname or IP Address)

RADIUS Server Secret:

☐ WPA

RADIUS Server: (Hostname or IP Address)

RADIUS Server Secret:

SSID Table

Delete	SSID	VLAN	Encryption	Authentication	Key Management	Native VLAN	Broadcast SSID
Delete	autoinstall	none	none	open	none		☒

117025

The Express Security page helps you configure basic security settings. You can use the web-browser interface's main Security pages to configure more advanced security settings.

Understanding Express Security Settings

The SSIDs that you create using the Express security page appear in the SSID table at the bottom of the page. You can create up to 16 SSIDs on the wireless device.

In Cisco IOS Release 12.3(7)JA, there is no default SSID. You must configure an SSID before client devices can associate to the access point/bridge.

Using VLANs

If you use VLANs on your wireless LAN and assign SSIDs to VLANs, you can create multiple SSIDs using any of the four security settings on the Express Security page. However, if you do not use VLANs on your wireless LAN, the security options that you can assign to SSIDs are limited because, on the Express Security page, encryption settings and authentication types are linked. Without VLANs, encryption settings (WEP and ciphers) apply to an interface such as the 2.4-GHz radio, and you cannot use more than one encryption setting on an interface. For example, when you create an SSID with static WEP with VLANs disabled, you cannot create additional SSIDs with WPA authentication because they use different encryption settings. If you find that the security setting for an SSID conflicts with another SSID, you can delete one or more SSIDs to eliminate the conflict.

Express Security Types

Table 2-2 describes the four security types that you can assign to an SSID.

Table 2-2 Security Types on Express Security Setup Page

Security Type	Description	Security Features Enabled
No Security	This is the least secure option. You should use this option only for SSIDs used in a public space and assign it to a VLAN that restricts access to your network.	None.
Static WEP Key	This option is more secure than no security. However, static WEP keys are vulnerable to attack. If you configure this setting, you should consider limiting association to the access point based on MAC address or, if your network does not have a RADIUS server, consider using an access point as a local authentication server.	Mandatory WEP encryption, no key management, and open authentication. In Root AP mode, client devices cannot associate using this SSID without a WEP key that matches the access point key.

Table 2-2 **Security Types on Express Security Setup Page (continued)**

Security Type	Description	Security Features Enabled
EAP Authentication	This option enables 802.1x authentication (such as LEAP, PEAP, EAP-TLS, EAP-GTC, EAP-SIM, and others) and requires you to enter the IP address and shared secret for an authentication server on your network (server authentication port 1645). Because 802.1x authentication provides dynamic encryption keys, you do not need to enter a WEP key.	Mandatory 802.1x authentication. In Root AP mode, client devices that associate using this SSID must perform 802.1x authentication.
WPA	Wi-Fi Protected Access (WPA) permits wireless access to users authenticated against a database through the services of an authentication server, then encrypts their IP traffic with stronger algorithms than those used in WEP. As with EAP authentication, you must enter the IP address and shared secret for an authentication server on your network (server authentication port 1645).	Mandatory WPA authentication. In Root AP mode, client devices that associate using this SSID must be WPA-capable.

Express Security Limitations

Because the Express Security page is designed for simple configuration of basic security, the options available are a subset of the access point/bridge's security capabilities. Keep these limitations in mind when using the Express Security page:

- If the **No VLAN** option is selected, the static WEP key can be configured once. If you select **Enable VLAN**, the static WEP key should be disabled.
- You cannot edit SSIDs. However, you can delete SSIDs and re-create them.
- You cannot assign SSIDs to specific radio interfaces. The SSIDs that you create are enabled on all radio interfaces. To assign SSIDs to specific radio interfaces, use the Security SSID Manager page.
- You cannot configure multiple authentication servers. To configure multiple authentication servers, use the Security Server Manager page.
- You cannot configure multiple WEP keys. To configure multiple WEP keys, use the Security Encryption Manager page.
- You cannot assign an SSID to a VLAN that is already configured on the access point/bridge. To assign an SSID to an existing VLAN, use the Security SSID Manager page.
- You cannot configure combinations of authentication types on the same SSID (for example, MAC address authentication and EAP authentication). To configure combinations of authentication types, use the Security SSID Manager page.

Using the Express Security Page

Follow these steps to create an SSID using the Express Security page:

-
- Step 1** Type the SSID in the SSID entry field. The SSID can contain up to 32 alphanumeric characters.
- Step 2** To broadcast the SSID in the wireless device beacon, check the Broadcast SSID in Beacon check box. The **Broadcast SSID in Beacon** setting is active only when the access point/bridge is in the Root AP mode. When you broadcast the SSID, devices that do not specify an SSID can associate to the access point/bridge when it is a root access point. This is a useful option for an SSID used by guests or by client devices in a public space. If you do not broadcast the SSID, client devices cannot associate to the access point unless their SSID matches this SSID. Only one SSID can be included in the beacon.
- Step 3** (Optional) Check the Enable VLAN ID check box and enter a VLAN number (1 through 4095) to assign the SSID to a VLAN. You cannot assign an SSID to an existing VLAN.
- Step 4** (Optional) Check the Native VLAN check box to mark the VLAN as the native VLAN.
- Step 5** Select the security setting for the SSID. The settings are listed in order of robustness, from No Security to WPA, which is the most secure setting. If you select EAP Authentication or WPA, enter the IP address and shared secret for the authentication server on your network.



Note

If you do not use VLANs on your wireless LAN, the security options that you can assign to multiple SSIDs are limited. See the [“Using VLANs” section on page 2-11](#) for details.

- Step 6** Click **Apply**. The SSID appears in the SSID table at the bottom of the page.
-

CLI Configuration Examples

The examples in this section show the CLI commands that are equivalent to creating SSIDs using each security type on the Express Security page. This section contains these example configurations:

- [Example: No Security, page 2-13](#)
- [Example: Static WEP, page 2-14](#)
- [Example: EAP Authentication, page 2-15](#)
- [Example: WPA, page 2-16](#)

Example: No Security

This example shows part of the configuration that results from using the Express Security page to create an SSID called *no_security_ssid*, including the SSID in the beacon, assigning it to VLAN 10, and selecting VLAN 10 as the native VLAN:

```
interface Dot11Radio0
  no ip address
  no ip route-cache
  !
  ssid no_security-ssid
    vlan 10
    authentication open
    guest-mode
  !
!
```

```

concatenation
speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
rts threshold 4000
station-role root
infrastructure-client
bridge-group 1
!
interface Dot11Radio0.10
encapsulation dot1Q 10
no ip route-cache
bridge-group 10
bridge-group 10 spanning-disabled
!
interface FastEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
bridge-group 1
!
interface FastEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
bridge-group 1

```

Example: Static WEP

This example shows part of the configuration that results from using the Express Security page to create an SSID called *static_wep_ssid*, excluding the SSID from the beacon, assigning the SSID to VLAN 20, selecting 3 as the key slot, and entering a 128-bit key:

```

interface Dot11Radio0
no ip address
no ip route-cache
!
encryption vlan 20 key 3 size 128bit 7 4E78330C1A841439656A9323F25A transmit-ke

encryption vlan 20 mode wep mandatory
!
ssid static_wep_ssid
vlan 20
authentication open
!
concatenation
speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
rts threshold 4000
station-role root
infrastructure-client
bridge-group 1
!
interface Dot11Radio0.20
encapsulation dot1Q 20
no ip route-cache
bridge-group 20
bridge-group 20 spanning-disabled
!
interface FastEthernet0
no ip address
no ip route-cache
duplex auto
speed auto

```

```
bridge-group 1
!
interface FastEthernet0.20
 encapsulation dot1Q 20
 no ip route-cache
 bridge-group 20
 bridge-group 20 spanning-disabled
```

Example: EAP Authentication

This example shows part of the configuration that results from using the Express Security page to create an SSID called *eap_ssid*, excluding the SSID from the beacon, and assigning the SSID to VLAN 30:

```
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption vlan 30 mode wep mandatory
 !
 ssid eap_ssid
  vlan 30
  authentication open eap eap_methods
  authentication network-eap eap_methods
 !
 speed basic-1.0 basic-2.0 basic-5.5 basic-11.0
 rts threshold 2312
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
 !
interface Dot11Radio0.30
 encapsulation dot1Q 30
 no ip route-cache
 bridge-group 30
 bridge-group 30 subscriber-loop-control
 bridge-group 30 block-unknown-source
 no bridge-group 30 source-learning
 no bridge-group 30 unicast-flooding
 bridge-group 30 spanning-disabled
 !
interface FastEthernet0
 mtu 1500
 no ip address
 ip mtu 1564
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
 !
interface FastEthernet0.30
 mtu 1500
 encapsulation dot1Q 30
 no ip route-cache
 bridge-group 30
 no bridge-group 30 source-learning
 bridge-group 30 spanning-disabled
 !
```

Example: WPA

This example shows part of the configuration that results from using the Express Security page to create an SSID called *wpa_ssid*, excluding the SSID from the beacon, and assigning the SSID to VLAN 40:

```
aaa new-model
!
!
aaa group server radius rad_eap
 server 10.91.104.92 auth-port 1645 acct-port 1646
!
aaa group server radius rad_mac
!
aaa group server radius rad_acct
!
aaa group server radius rad_admin
!
aaa group server tacacs+ tac_admin
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authorization exec default local
aaa authorization ipmobile default group rad_pmip
aaa accounting network acct_methods start-stop group rad_acct
aaa session-id common
!
!
bridge irb
!
!
interface Dot11Radio0
 no ip address
 no ip route-cache
!
 encryption vlan 40 mode ciphers tkip
!
 ssid wpa_ssid
  vlan 40
  authentication open eap eap_methods
  authentication network-eap eap_methods
  authentication key-management wpa
!
 concatenation
 speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48 54.0
 rts threshold 4000
 station-role root
 infrastructure-client
 bridge-group 1
!
interface Dot11Radio0.40
 encapsulation dot1Q 40
 no ip route-cache
 bridge-group 40
!
interface FastEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
```



```

!
interface FastEthernet0.40
 encapsulation dot1Q 40
 no ip route-cache
 bridge-group 40
!
ip http server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
/122-15.JA/1100
ip radius source-interface BVI1
radius-server attribute 32 include-in-access-req format %h
radius-server host 10.91.104.92 auth-port 1645 acct-port 1646 key 7 135445415F59
radius-server authorization permit missing Service-Type
radius-server vsa send accounting
bridge 1 route ip
!
!
!
line con 0
line vty 5 15
!
end

```

Using the IP Setup Utility

IPSU enables you to find the access point/bridge's IP address when it has been assigned by a DHCP server. access point/bridge. This section explains how to download the utility from Cisco.com and install it, how to use it to find the access point/bridge's IP address.



Note

IPSU can be used only on the following operating systems: Windows 95, 98, NT, 2000, ME, or XP.

Obtaining and Installing IPSU

IPSU is available on the Cisco web site. Follow these steps to obtain and install IPSU:

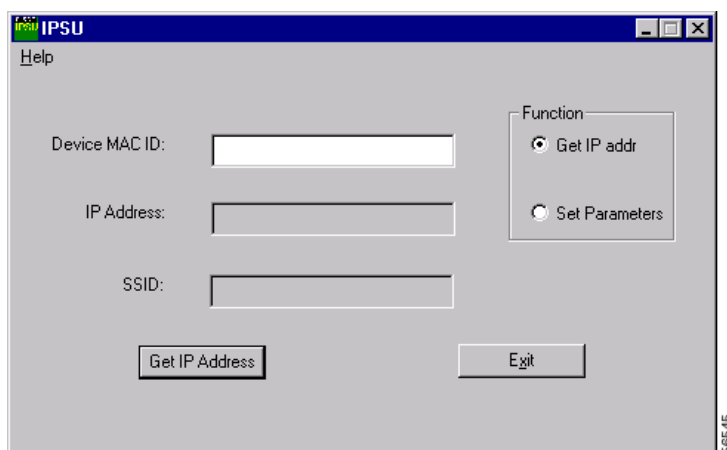
- Step 1** Use your Internet browser to access the Cisco Software Center at the following URL:
<http://www.cisco.com/cisco/software/navigator.html>
- Step 2** Click **Option #2: Aironet Wireless Software Display Tables**. The Wireless Software page appears.
- Step 3** Click **Cisco Aironet 1300 Series**. The Software Download page appears.
- Step 4** Click the file **IPSUvxxxxxx.exe**. The *xxxxxx* identifies the software package version number.
- Step 5** Read and accept the terms and conditions of the Software License Agreement.
- Step 6** Download and save the file to a temporary directory on your hard drive and then exit the Internet browser.
- Step 7** Double-click **IPSUvxxxxxx.exe** in the temporary directory to expand the file.
- Step 8** Double-click **Setup.exe** and follow the steps provided by the installation wizard to install IPSU.
The IPSU icon appears on your computer desktop.

Using IPSU to Find the Access Point/Bridge's IP Address

If your bridge receives an IP address from a DHCP server, you can use IPSU to find its IP address. Because IPSU sends a reverse-ARP request based on the bridge MAC address, you must run IPSU from a computer on the same subnet as the bridge. Follow these steps to find the bridge's IP address:

- Step 1** Double-click the **IPSU** icon on your computer desktop to start the utility. The IPSU screen appears (see [Figure 2-5](#)).

Figure 2-5 *IPSU Get IP Address Screen*



- Step 2** When the utility window opens, make sure the *Get IP addr* radio button in the Function box is selected.
- Step 3** Enter the access point/bridge's MAC address in the Device MAC ID field. The access point/bridge's MAC address is printed on the label on the bottom of the unit. It should contain six pairs of hexadecimal digits. Your access point/bridge's MAC address might look like the following example:

000164xxxxxx



Note The MAC address field is not case-sensitive.

- Step 4** Click **Get IP Address**.
- Step 5** When the access point/bridge's IP address appears in the IP Address field, write it down.

Using a Telnet Session to Access the CLI

Follow these steps to browse to access the CLI using a Telnet session. These steps are for a PC running Microsoft Windows with a Telnet terminal application. Check your PC operating instructions for detailed instructions for your operating system.

Step 1 Select **Start > 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 drop-down menus. To start the Telnet session in Windows 2000, type **open** followed by the access point/bridge's IP address.

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

Resetting the Access Point/Bridge to Default Settings

You can use the web-browser interface or the CLI to reset the access point/bridge to a factory default configuration.



Note The following steps reset all configuration settings to factory defaults, including passwords, WEP keys, the IP address (if desired), and the SSID.

Using the Web-Browser Interface

Follow the steps below to delete the current configuration and return all access point/bridge settings to the factory defaults using the Web-browser interface.

Step 1 Open your Internet browser.

Step 2 Enter the access point/bridge's IP address in the browser address or location line and press **Enter**. An Enter Network Password screen appears.

Step 3 Enter your username (default *Cisco*) in the User Name field.

Step 4 Enter the access point/bridge password (default *Cisco*) in the Password field and press **Enter**. The Summary Status page appears.

Step 5 Click **System Software** and the System Software screen appears.

Step 6 Click **System Configuration** and the System Configuration screen appears.

Step 7 Click one of the following:

- a. **Reset to Defaults**—resets all settings to factory defaults, including the IP address.
- b. **Reset to Defaults (Except IP)**—resets all settings except the IP address to factory defaults.

- Step 8** Click **Apply**.
- Step 9** Click **Restart**.
- Step 10** After the access point/bridge reboots, you can reconfigure the access point/bridge by using the Web-browser interface or the CLI (refer to the *Cisco IOS Software Configuration Guide for Cisco Aironet Bridges* or to the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*).

Using the CLI



Caution

You should never delete any of the system files prior to resetting defaults or reloading software.

If you want to reset the access point/bridge to its default settings and a static IP address, use the *write erase* or *erase /all nvram* command. If you want to erase everything including the static IP address, in addition to the above commands, use the *erase* and *erase boot static-ipaddr static-ipmask* command.

From the privileged EXEC mode, you can reset the access point/bridge configuration to factory default values using the CLI by following these steps:

- Step 1** Enter **erase nvram:** to erase all NVRAM files including the startup configuration.



Note

The **erase nvram** command does not erase a static IP address.

- Step 2** Follow the step below to erase a static IP address and subnet mask. Otherwise, go to step 3.

- a.** Enter **erase boot static ip-address static-ipmask**.

- Step 3** Enter **Y** when the following CLI message displays: *Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]*.

- Step 4** Enter **reload** when the following CLI message displays: *Erase of nvram: complete*. This command reloads the operating system.

- Step 5** Enter **Y** when the following CLI message displays: *Proceed with reload? [confirm]*.



Caution

Do not interrupt the boot process to avoid damaging the configuration file. Wait until the access point/bridge Install Mode LED begins to blink green before continuing with CLI configuration changes. You can also see the following CLI message when the load process has finished: *Line protocol on Interface Dot11Radio0, changed state to up*.

- Step 6** After the access point/bridge reboots, you can reconfigure the access point/bridge by using the Web-browser interface if you previously assigned a static IP address, or the CLI if you did not.

The access point/bridge is configured with the factory default values including the IP address (set to receive an IP address using DHCP). To obtain the access point/bridge's new IP address, you can use the *show interface bvi1* CLI command.



Using the Web-Browser Interface

This chapter describes the web-browser interface that you can use to configure the access point/bridge. It contains these sections:

- [Using the Web-Browser Interface for the First Time, page 3-2](#)
- [Using the Management Pages in the Web-Browser Interface, page 3-2](#)
- [Enabling HTTPS for Secure Browsing, page 3-4](#)
- [Using Online Help, page 3-12](#)
- [Disabling the Web-Browser Interface, page 3-14](#)

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



Note

The access point/bridge web-browser interface is fully compatible with these browsers: Microsoft Internet Explorer versions 6.0 on Windows 98, 2000, and XP platforms, and with Netscape version 7.0 on Windows 98, Windows 2000, and Solaris platforms.



Note

Avoid using the CLI and the web-browser interfaces to configure the access point/bridge. Use one or the other. If you configure the access point/bridge using the CLI, the web-browser interface might display an inaccurate interpretation of the configuration. However, the inaccuracy does not necessarily mean that the access point/bridge is misconfigured.

Using the Web-Browser Interface for the First Time

Use the access point/bridge's IP address to browse to the management system. See the [“Obtaining and Assigning an IP Address” section on page 2-2](#) for instructions on assigning an IP address to the access point/bridge.

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

-
Step 1	Start the browser.
Step 2	Enter the access point/bridge's IP address in the browser Location field (Netscape Communicator) or Address field (Internet Explorer) and press Enter .
Step 3	Enter the administrator username and password and press Enter . The default username is <i>Cisco</i> and the default password is <i>Cisco</i> . 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. A navigation bar is on the left side of the page, and configuration action buttons appear at the bottom. You use the navigation bar to browse to other management pages, and you use the configuration action buttons to save or cancel changes to the configuration.

**Note**

It is important to remember that clicking your browser's **Back** button returns you to the previous page without saving any changes you have made. Clicking **Cancel** cancels any changes you made on the page and keeps you on that page. Changes are only applied when you click **Apply**.

[Figure 3-1](#) shows the web-browser interface home page.

Figure 3-1 Web-Browser Interface Home Page

Hostname bridge bridge uptime is 47 minutes

Home: Summary Status

Association

Clients: 0 Infrastructure clients: 0

Network Identity

IP Address: 10.0.0.1
MAC Address: 0005.9a3f.57f4

Network Interfaces

Interface	MAC Address	Transmission Rate
FastEthernet	0005.9a3f.57f4	100Mb/s
Radio0-802.11G	000e.8319.2800	54.0Mb/s

Event Log

Time	Severity	Description
Mar 1 00:01:40.876	Notification	Line protocol on Interface Dot11Radio0, changed state to up
Mar 1 00:01:39.882	Error	Interface Dot11Radio0, changed state to up
Mar 1 00:01:39.875	Warning	Root selected
Mar 1 00:00:50.307	Warning	Interface Dot11Radio0, cannot associate: No matching SSID
Mar 1 00:00:40.355	Notification	Interface Dot11Radio0, changed state to reset
Mar 1 00:00:40.354	Warning	Non-root - scanning for root
Mar 1 00:00:34.307	Information	Interface Dot11Radio0, frequency 2447 selected
Mar 1 00:00:26.409	Notification	Line protocol on Interface Dot11Radio0, changed state to down
Mar 1 00:00:26.375	Notification	Line protocol on Interface BVI1, changed state to up
Mar 1 00:00:25.448	Notification	Interface Dot11Radio0, changed state to administratively down

Refresh

117034

Using Action Buttons

Table 3-1 lists the page links and buttons that appear on most management pages.

Table 3-1 Common Buttons on Management Pages

Button/Link	Description
Navigation Links	
Home	Displays access point/bridge status page with information on the number of radio devices associated to the access point/bridge, the status of the Ethernet and radio interfaces, and a list of recent access point/bridge activity.
Express Setup	Displays the Express Setup page that includes basic settings such as system name, IP address, and SSID.
Express Security	Displays the Express Security page from which you can select basic security settings (no security, static WEP key, EAP authentication, or WPA).
Network Map	Displays a list of infrastructure devices on your wireless LAN.
Association	Displays a list of all devices on your wireless LAN, listing their system names, network roles, and parent-client relationships.

Table 3-1 Common Buttons on Management Pages (continued)

Button/Link	Description
Network Interfaces	Displays status and statistics for the Ethernet and radio interfaces and provides links to configuration pages for each interface.
Security	Displays a summary of security settings and provides links to security configuration pages.
Services	Displays status for several access point/bridge features and links to configuration pages for Telnet/SSH, CDP, domain name server, filters, proxy Mobile IP, QoS, SNMP, SNTP, and VLANs.
Wireless Services	Displays the Wireless Domain Services Status page and provides access to the AP and Wireless Domain Services (WDS) pages.
System Software	Displays the version number of the firmware that the access point/bridge is running and provides links to configuration pages for upgrading and managing firmware.
Event Log	Displays the access point/bridge event log and provides links to configuration pages where you can select events to be included in traps, set event severity levels, and set notification methods.
Configuration Action Buttons	
Apply	Saves changes made on the page and remains on the page.
Refresh	Updates status information or statistics displayed on a page.
Cancel	Discards changes to the page and remains on the page.
Back	Discards any changes made to the page and returns to the previous page.

Character Restrictions in Entry Fields

Because the 1300 series access point/bridge uses Cisco IOS software, there are certain characters that you cannot use in the entry fields on the web-browser interface. You cannot use these characters in entry fields:

“
]
+
/
Tab
Trailing space

Enabling HTTPS for Secure Browsing

You can protect communication with the access point/bridge web-browser interface by enabling HTTPS. HTTPS protects HTTP browser sessions by using the Secure Socket Layer (SSL) protocol.

**Note**

When you enable HTTPS, your browser might lose its connection to the access point/bridge. If you lose the connection, change the URL in your browser's address line from `http://ip_address` to `https://ip_address` and log into the access point again.

**Note**

When you enable HTTPS, most browsers prompt you for approval each time you browse to a device that does not have a fully qualified domain name (FQDN). To avoid the approval prompts, complete [Step 2](#) through [Step 9](#) in these instructions to create an FQDN for the access point. However, if you do not want to create an FQDN, skip to [Step 10](#).

Follow these steps to create an FQDN and enable HTTPS:

Step 1 If your browser uses popup-blocking software, disable the popup-blocking feature.

Step 2 Browse to the Express Setup page. [Figure 3-2](#) shows the Express Setup page.

Figure 3-2 Express Setup Page

HOME
EXPRESS SET-UP
EXPRESS SECURITY
NETWORK MAP
ASSOCIATION
NETWORK INTERFACES
SECURITY
SERVICES
WIRELESS SERVICES
SYSTEM SOFTWARE
EVENT LOG

Hostname root root uptime is 5 days, 22 hours, 47 minutes

Express Set-Up

Host Name:

MAC Address: 0012.016c.0240

Configuration Server Protocol: ☐ DHCP ☒ Static IP

IP Address:

IP Subnet Mask:

Default Gateway:

SNMP Community:

☒ Read-Only ☐ Read-Write

Radio0-802.11G

Role in Radio Network: ☒ Root ☐ Non-Root ☐ Install-Mode
☐ Non-Root with Clients
☐ Root AP ☐ Repeater AP
☐ Workgroup Bridge

Optimize Radio Network for: ☐ Throughput ☐ Range ☒ Default ☐ Custom

Aironet Extensions: ☒ Enable ☐ Disable

Apply Cancel

Step 3 Enter a name for the access point/bridge in the System Name field and click **Apply**.

Step 4 Browse to the Services – DNS page. [Figure 3-3](#) shows the Services – DNS page.

Figure 3-3 Services – DNS Page

Step 5 Select **Enable** for Domain Name System.

Step 6 In the Domain Name field, enter your company's domain name. At Cisco Systems, for example, the domain name is *cisco.com*.

Step 7 Enter at least one IP address for your DNS server in the Name Server IP Addresses entry fields.

Step 8 Click **Apply**. The access point/bridge's FQDN is a combination of the system name and the domain name. For example, if your system name is *br 1310* and your domain name is *company.com*, the FQDN is *br1310.company.com*.

Step 9 Enter the FQDN on your DNS server.

**Tip**

If you do not have a DNS server, you can register the access point/bridge's FQDN with a dynamic DNS service. Search the Internet for *dynamic DNS* to find a fee-based DNS service.

Step 10 Browse to the Services: HTTP Web Server page. [Figure 3-4](#) shows the HTTP Web Server page:

Figure 3-4 Services: HTTP Web Server Page

Hostname root root uptime is 5 days, 22 hours, 27 minutes

Services: HTTP - Web Server

Web-based Configuration Management:

- ☒ Enable Standard (HTTP) Browsing
- ☐ Enable Secure (HTTPS) Browsing
- ☐ Disable Web-based Management

System Name:

Domain Name:

HTTP Port: (1025-65535 or default 80)

HTTPS Port: (1025-65535 or default 443)

Help Root URL: (Set to default by clearing textbox)

Target Help URL:

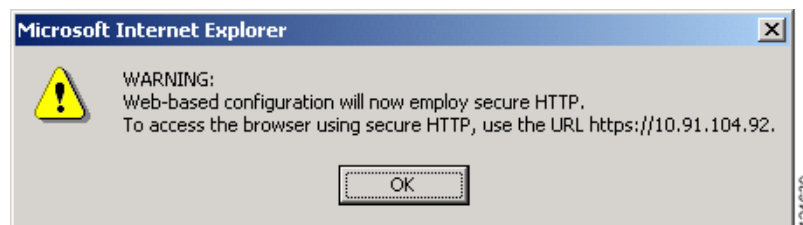
Apply **Cancel**

Step 11 Select the Enable Secure (HTTPS) Browsing check box and click **Apply**.



Note Although you can enable both standard HTTP and HTTPS, Cisco recommends that you enable one or the other.

A warning window appears stating that you will use HTTPS to browse to the access point. The window also instructs you to change the URL that you use to browse to the access point/bridge from *http* to *https*. Figure 3-5 shows the warning window:

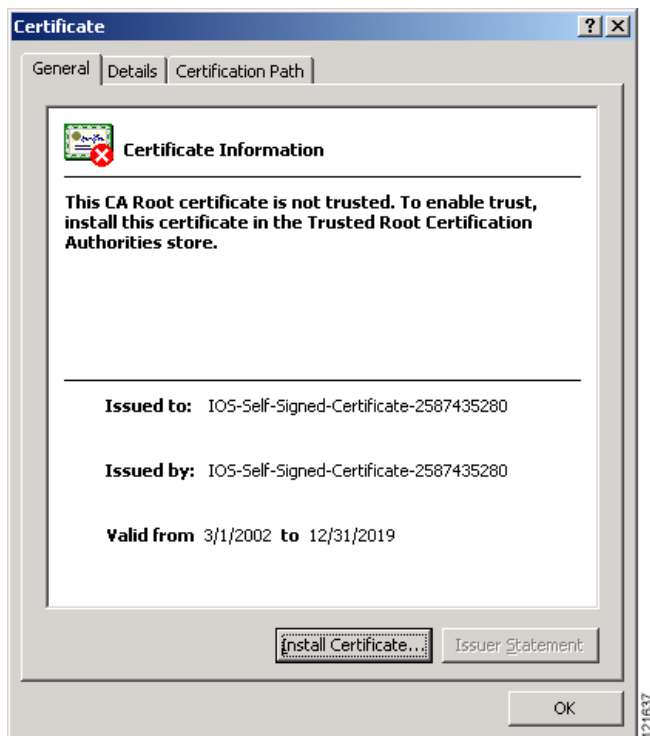
Figure 3-5 HTTPS Warning Window

Step 12 Click **OK**. The address in your browser's address line changes from **http://ip-address** to **https://ip-address**.

Step 13 Another warning window appears stating that the access point's security certificate is valid but is not from a known source. However, you can accept the certificate with confidence because the site in question is your own access point. Figure 3-6 shows the certificate warning window:

Figure 3-6 Certificate Warning Window

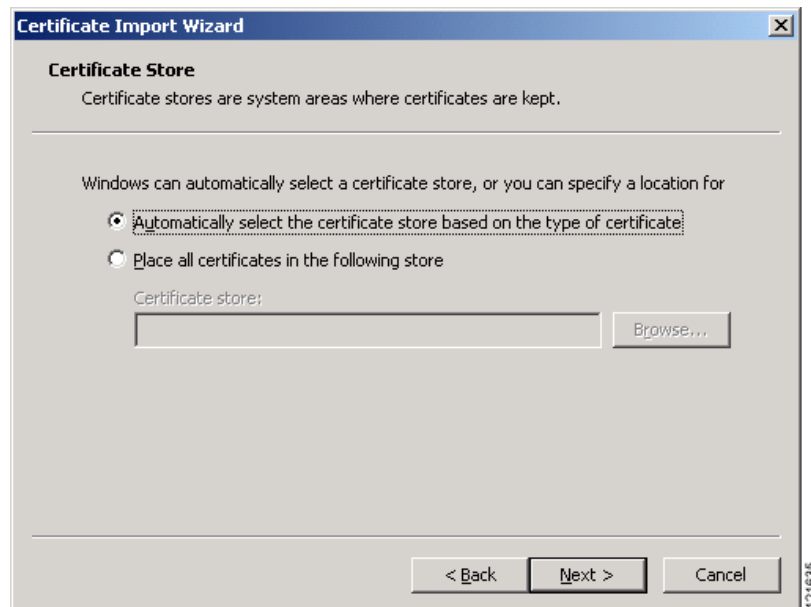
- Step 14** Click **View Certificate** to accept the certificate before proceeding. (To proceed without accepting the certificate, click **Yes**, and skip to [Step 23](#) in these instructions.) [Figure 3-7](#) shows the Certificate window.

Figure 3-7 Certificate Window

- Step 15** On the Certificate window, click **Install Certificate**. The Microsoft Windows Certificate Import Wizard appears. [Figure 3-8](#) shows the Certificate Import Wizard window.

Figure 3-8 Certificate Import Wizard Window

- Step 16** Click **Next**. The next window asks where you want to store the certificate. Cisco recommends that you use the default storage area on your system. [Figure 3-9](#) shows the window that asks about the certificate storage area.

Figure 3-9 Certificate Storage Area Window

- Step 17** Click **Next** to accept the default storage area. A window appears that states that you successfully imported the certificate. [Figure 3-10](#) shows the completion window.

Figure 3-10 Certificate Completion Window

Step 18 Click **Finish**. Windows displays a final security warning. [Figure 3-11](#) shows the security warning.

Figure 3-11 Certificate Security Warning

Step 19 Click **Yes**. Windows displays another window stating that the installation is successful. [Figure 3-12](#) shows the completion window.

Figure 3-12 Import Successful Window

- Step 20** Click **OK**.
- Step 21** On the Certificate window shown in [Figure 3-7](#), which is still displayed, click **OK**.
- Step 22** On the Security Alert window shown in [Figure 3-6](#), click **Yes**.
- Step 23** The access point login window appears and you must log into the access point again. The default user name is *Cisco* (case-sensitive) and the default password is *Cisco* (case-sensitive).

CLI Configuration Example

This example shows the CLI commands that are equivalent to the steps listed in the [“Using Online Help” section on page 3-12](#):

```
ap# configure terminal
ap(config)# hostname br1310
ap(config)# ip domain name company.com
ap(config)# ip name-server 10.91.107.18
ap(config)# ip http secure-server
ap(config)# end
```

In this example, the access point system name is *br1310*, the domain name is *company.com*, and the IP address of the DNS server is 10.91.107.18.

For complete descriptions of the commands used in this example, consult the Cisco IOS Commands Master List, Release 12.3. Click this link to browse to the master list of commands:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123mindx/index.htm>

Deleting an HTTPS Certificate

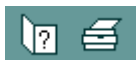
The access point generates a certificate automatically when you enable HTTPS. However, if you need to change the access point's fully qualified domain name (FQDN) or you need to add an FQDN after enabling HTTPS, you might need to delete the certificate. Follow these steps:

- Step 1** Browse to the Services: HTTP Web Server page.
- Step 2** Uncheck the **Enable Secure (HTTPS) Browsing** check box to disable HTTPS.
- Step 3** Click **Delete Certificate** to delete the certificate.
- Step 4** Re-enable HTTPS. The access point generates a new certificate using the new FQDN.

Using Online Help

Click the help icon at the top of any page in the web-browser interface to display online help. [Figure 3-13](#) shows the print and help icons.

Figure 3-13 *Print and Help Icons*



When a help page appears in a new browser window, use the Select a topic drop-down menu to display the help index or instructions for common configuration tasks, such as configuring VLANs.

Changing the Location of Help Files

Cisco maintains up-to-date HTML help files for access points and bridges on the Cisco web site. By default, the access point/bridge opens a help file on Cisco.com when you click the help button on the access point web-browser interface. However, you can install the help files on your network so your devices can access them there. Follow these steps to install the help files locally:

-
- Step 1** Download the help files from the Software Center on Cisco.com. Click this link to browse to the Software Center's Wireless Software page:
- <http://www.cisco.com/cisco/software/navigator.html>
- Select the help files that match the software version on your access point.
- Step 2** Unzip the help files on your network in a directory accessible to your access point/bridge. When you unzip the help files, the HTML help pages are stored in a folder named according to the help version number and access point model number.
- Step 3** Browse to the Services: HTTP Web Server page in the access point web-browser interface. [Figure 3-14](#) shows the HTTP Web Server page:

Figure 3-14 HTTP Web Server Page

Hostname root root uptime is 5 days, 22 hours, 27 minutes

Services: HTTP- Web Server

Web-based Configuration Management:

- ☒ Enable Standard (HTTP) Browsing
- ☐ Enable Secure (HTTPS) Browsing
- ☐ Disable Web-based Management

System Name:

Domain Name:

HTTP Port: (1025-65535 or default 80)

HTTPS Port: (1025-65535 or default 443)

Help Root URL: (Set to default by clearing textbox)

Target Help URL:

Apply Cancel

- Step 4** In the Default Help Root URL entry field, enter the complete path to the location where you unzipped the help files. When you click the access point help button, the access point automatically appends the help version number and model number to the path that you enter.

**Note**

Do not add the help version number and device model number to the Default Help Root URL entry. The access point automatically adds the help version and model number to the help root URL.

If you unzip the help files on your network file server at `//myserver/myhelp`, your Default Help Root URL looks like this:

`http://myserver/myhelp`

Table 3-2 shows an example help location and Help Root URL for an 1100 series access point.

Table 3-2 Example Help Root URL and Help Location

Files Unzipped at This Location	Default Help Root URL	Actual Location of Help Files
<code>//myserver/myhelp</code>	<code>http://myserver/myhelp</code>	<code>//myserver/myhelp/123-02.JA/1100</code>

- Step 5** Click **Apply**.

Disabling the Web-Browser Interface

To prevent all use of the web-browser interface, select the **Disable Web-Based Management** check box on the Services: HTTP-Web Server page and click **Apply**. Figure 3-15 shows the Services: HTTP-Web Server page.

Figure 3-15 Services: HTTP-Web Server Page

HOME

EXPRESS SET-UP

EXPRESS SECURITY

NETWORK MAP +

ASSOCIATION +

NETWORK INTERFACES +

SECURITY +

SERVICES

Telnet/SSH

CDP

DNS

Filters

HTTP

QoS

SNMP

SNTP

VLAN

STP

ARP Caching

WIRELESS SERVICES +

SYSTEM SOFTWARE +

EVENT LOG +

Hostname root

root uptime is 5 days, 22 hours, 27 minutes

Services: HTTP-Web Server

Web-based Configuration Management:

☒ Enable Standard (HTTP) Browsing

☐ Enable Secure (HTTPS) Browsing

☐ Disable Web-based Management

System Name:

root

Domain Name:

HTTP Port:

80

(1025-65535 or default 80)

HTTPS Port:

443

(1025-65535 or default 443)

Help Root URL: (Set to default by clearing textbox)

http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag

Target Help URL:

http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag/123-04.JA/1100

Apply

Cancel

To re-enable the web-browser interface, enter this global configuration command on the access point CLI:

```
ap(config)# ip http server
```



Using the Command-Line Interface

This chapter describes the IOS command-line interface (CLI) that you can use to configure your access point/bridge. It contains these sections:

- [IOS Command Modes, page 4-2](#)
- [Getting Help, page 4-3](#)
- [Abbreviating Commands, page 4-3](#)
- [Using no and default Forms of Commands, page 4-3](#)
- [Understanding CLI Messages, page 4-4](#)
- [Using Command History, page 4-4](#)
- [Using Editing Features, page 4-5](#)
- [Searching and Filtering Output of show and more Commands, page 4-8](#)
- [Accessing the CLI, page 4-8](#)

IOS Command Modes

The Cisco IOS user interface is divided into many different modes. The commands available to you depend on which mode you are currently in. Enter a question mark (?) at the system prompt to obtain a list of commands available for each command mode.

When you start a session on the access point/bridge, you begin in user mode, often called *user EXEC mode*. Only a limited subset of the commands are available in user EXEC mode. For example, most of the user EXEC commands are one-time commands, such as **show** commands, which show the current configuration status, and **clear** commands, which clear counters or interfaces. The user EXEC commands are not saved when the access point/bridge reboots.

To have access to all commands, you must enter privileged EXEC mode. Normally, you must enter a password to enter privileged EXEC mode. From this mode, you must enter privileged EXEC mode before you can enter the global configuration mode.

Using the configuration modes (global, interface, and line), you can make changes to the running configuration. If you save the configuration, these commands are stored and used when the access point/bridge reboots. To access the various configuration modes, you must start at global configuration mode. From global configuration mode, you can enter interface configuration mode and line configuration mode.

[Table 4-1](#) describes the main command modes, how to access each one, the prompt you see in that mode, and how to exit the mode. The examples in the table use the host name *BR*.

Table 4-1 Command Mode Summary

Mode	Access Method	Prompt	Exit Method	About This Mode
User EXEC	Begin a session with your access point/bridge.	bridge>	Enter logout or quit .	Use this mode to: • Change terminal settings • Perform basic tests • Display system information
Privileged EXEC	While in user EXEC mode, enter the enable command.	bridge#	Enter disable to exit.	Use this mode to verify commands. Use a password to protect access to this mode.
Global configuration	While in privileged EXEC mode, enter the configure command.	bridge(config)#	To exit to privileged EXEC mode, enter exit or end , or press Ctrl-Z .	Use this mode to configure parameters that apply to the entire access point/bridge.
Interface configuration	While in global configuration mode, enter the interface command (with a specific interface).	bridge(config-if)#	To exit to global configuration mode, enter exit . To return to privileged EXEC mode, press Ctrl-Z or enter end .	Use this mode to configure parameters for the Ethernet and radio interfaces. The 2.4-GHz radio is radio 0.

Getting Help

You can enter a question mark (?) at the system prompt to display a list of commands available for each command mode. You can also obtain a list of associated keywords and arguments for any command, as shown in [Table 4-2](#).

Table 4-2 Help Summary

Command	Purpose
help	Obtains a brief description of the help system in any command mode.
<i>abbreviated-command-entry?</i>	Obtains a list of commands that begin with a particular character string. For example: bridge# di? dir disable disconnect
<i>abbreviated-command-entry</i> <Tab>	Completes a partial command name. For example: bridge# sh conf <tab> bridge# show configuration
?	Lists all commands available for a particular command mode. For example: bridge> ?
<i>command ?</i>	Lists the associated keywords for a command. For example: bridge> show ?
<i>command keyword ?</i>	Lists the associated arguments for a keyword. For example: bridge(config)# cdp holdtime ? <10-255> Length of time (in sec) that receiver must keep this packet

Abbreviating Commands

You have to enter only enough characters for the access point/bridge to recognize the command as unique. This example shows how to enter the **show configuration** privileged EXEC command:

```
bridge# show conf
```

Using no and default Forms of Commands

Most configuration commands also have a **no** form. In general, use the **no** form to disable a feature or function or reverse the action of a command. For example, the **no shutdown** interface configuration command reverses the shutdown of an interface. Use the command without the keyword **no** to re-enable a disabled feature or to enable a feature that is disabled by default.

Configuration commands can also have a **default** form. The **default** form of a command returns the command setting to its default. Most commands are disabled by default, so the **default** form is the same as the **no** form. However, some commands are enabled by default and have variables set to certain default values. In these cases, the **default** command enables the command and sets variables to their default values.

Understanding CLI Messages

Table 4-3 lists some error messages that you might encounter while using the CLI to configure your access point/bridge.

Table 4-3 Common CLI Error Messages

Error Message	Meaning	How to Get Help
% Ambiguous command: "show con"	You did not enter enough characters for your access point/bridge to recognize the command.	Re-enter the command followed by a question mark (?) with a space between the command and the question mark. The possible keywords that you can enter with the command are displayed.
% Incomplete command.	You did not enter all the keywords or values required by this command.	Re-enter the command followed by a question mark (?) with a space between the command and the question mark. The possible keywords that you can enter with the command are displayed.
% Invalid input detected at '^' marker.	You entered the command incorrectly. The caret (^) marks the point of the error.	Enter a question mark (?) to display all the commands that are available in this command mode. The possible keywords that you can enter with the command are displayed.

Using Command History

The IOS provides a history or record of commands that you have entered. This feature is particularly useful for recalling long or complex commands or entries, including access lists. You can customize the command history feature to suit your needs as described in these sections:

- [Changing the Command History Buffer Size, page 4-4](#)
- [Recalling Commands, page 4-5](#)
- [Disabling the Command History Feature, page 4-5](#)

Changing the Command History Buffer Size

By default, the access point/bridge records ten command lines in its history buffer. Beginning in privileged EXEC mode, enter this command to change the number of command lines that the access point/bridge records during the current terminal session:

```
ap# terminal history [size number-of-lines]
```

The range is from 0 to 256.

Beginning in line configuration mode, enter this command to configure the number of command lines the access point/bridge records for all sessions on a particular line:

```
ap(config-line)# history [size number-of-lines]
```

The range is from 0 to 256.

Recalling Commands

To recall commands from the history buffer, perform one of the actions listed in [Table 4-4](#):

Table 4-4 *Recalling Commands*

Action ¹	Result
Press Ctrl-P or the up arrow key.	Recall commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Press Ctrl-N or the down arrow key.	Return to more recent commands in the history buffer after recalling commands with Ctrl-P or the up arrow key. Repeat the key sequence to recall successively more recent commands.
show history	While in privileged EXEC mode, list the last several commands that you just entered. The number of commands that are displayed is determined by the setting of the terminal history global configuration command and history line configuration command.

1. The arrow keys function only on ANSI-compatible terminals such as VT100s.

Disabling the Command History Feature

The command history feature is automatically enabled.

To disable the feature during the current terminal session, enter the **terminal no history** privileged EXEC command.

To disable command history for the line, enter the **no history** line configuration command.

Using Editing Features

This section describes the editing features that can help you manipulate the command line. It contains these sections:

- [Enabling and Disabling Editing Features, page 4-6](#)
- [Editing Commands Through Keystrokes, page 4-6](#)
- [Editing Command Lines that Wrap, page 4-7](#)

Enabling and Disabling Editing Features

Although enhanced editing mode is automatically enabled, you can disable it.

To re-enable the enhanced editing mode for the current terminal session, enter this command in privileged EXEC mode:

```
ap# terminal editing
```

To reconfigure a specific line to have enhanced editing mode, enter this command in line configuration mode:

```
ap(config-line)# editing
```

To globally disable enhanced editing mode, enter this command in line configuration mode:

```
ap(config-line)# no editing
```

Editing Commands Through Keystrokes

Table 4-5 shows the keystrokes that you need to edit command lines.

Table 4-5 *Editing Commands Through Keystrokes*

Capability	Keystroke ¹	Purpose
Move around the command line to make changes or corrections.	Ctrl-B or the left arrow key	Move the cursor back one character.
	Ctrl-F or the right arrow key	Move the cursor forward one character.
	Ctrl-A	Move the cursor to the beginning of the command line.
	Ctrl-E	Move the cursor to the end of the command line.
	Esc B	Move the cursor back one word.
	Esc F	Move the cursor forward one word.
	Ctrl-T	Transpose the character to the left of the cursor with the character located at the cursor.
Recall commands from the buffer and paste them in the command line. The access point/bridge provides a buffer with the last ten items that you deleted.	Ctrl-Y	Recall the most recent entry in the buffer.
	Esc Y	Recall the next buffer entry. The buffer contains only the last 10 items that you have deleted or cut. If you press Esc Y more than ten times, you cycle to the first buffer entry.
Delete entries if you make a mistake or change your mind.	Delete or Backspace	Erase the character to the left of the cursor.
	Ctrl-D	Delete the character at the cursor.
	Ctrl-K	Delete all characters from the cursor to the end of the command line.
	Ctrl-U or Ctrl-X	Delete all characters from the cursor to the beginning of the command line.
	Ctrl-W	Delete the word to the left of the cursor.
	Esc D	Delete from the cursor to the end of the word.

Table 4-5 *Editing Commands Through Keystrokes (continued)*

Capability	Keystroke ¹	Purpose
Capitalize or lowercase words or capitalize a set of letters.	Esc C	Capitalize at the cursor.
	Esc L	Change the word at the cursor to lowercase.
	Esc U	Capitalize letters from the cursor to the end of the word.
Designate a particular keystroke as an executable command, perhaps as a shortcut.	Ctrl-V or Esc Q	
Scroll down a line or screen on displays that are longer than the terminal screen can display. Note The <code>More</code> prompt appears for output that has more lines than can be displayed on the terminal screen, including show command output. You can use the Return and Space bar keystrokes whenever you see the <code>More</code> prompt.	Return	Scroll down one line.
	Space	Scroll down one screen.
Redisplay the current command line if the access point/bridge suddenly sends a message to your screen.	Ctrl-L or Ctrl-R	Redisplay the current command line.

1. The arrow keys function only on ANSI-compatible terminals such as VT100s.

Editing Command Lines that Wrap

You can use a wraparound feature for commands that extend beyond a single line on the screen. When the cursor reaches the right margin, the command line shifts ten spaces to the left. You cannot see the first ten characters of the line, but you can scroll back and check the syntax at the beginning of the command.

To scroll back to the beginning of the command entry, press **Ctrl-B** or the left arrow key repeatedly. You can also press **Ctrl-A** to immediately move to the beginning of the line.



Note

The arrow keys function only on ANSI-compatible terminals such as VT100s.

In this example, the **access-list** global configuration command entry extends beyond one line. When the cursor first reaches the end of the line, the line is shifted ten spaces to the left and redisplayed. The dollar sign (\$) shows that the line has been scrolled to the left. Each time the cursor reaches the end of the line, the line is again shifted ten spaces to the left.

```
ap(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1
ap(config)# $ 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.25
ap(config)# $t tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq
ap(config)# $108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq 45
```

After you complete the entry, press **Ctrl-A** to check the complete syntax before pressing the **Return** key to execute the command. The dollar sign (\$) appears at the end of the line to show that the line has been scrolled to the right:

```
ap(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1$
```

The software assumes you have a terminal screen that is 80 columns wide. If you have a width other than that, use the **terminal width** privileged EXEC command to set the width of your terminal.

Use line wrapping with the command history feature to recall and modify previous complex command entries. For information about recalling previous command entries, see the [“Editing Commands Through Keystrokes”](#) section on page 4-6.

Searching and Filtering Output of show and more Commands

You can search and filter the output for **show** and **more** commands. This is useful when you need to sort through large amounts of output or if you want to exclude output that you do not need to see.

To use this functionality, enter a **show** or **more** command followed by the *pipe* character (|), one of the keywords **begin**, **include**, or **exclude**, and an expression that you want to search for or filter out:

```
command | {begin | include | exclude} regular-expression
```

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

This example shows how to include in the output display only lines where the expression *protocol* appears:

```
ap# show interfaces | include protocol
Vlan1 is up, line protocol is up
Vlan10 is up, line protocol is down
GigabitEthernet0/1 is up, line protocol is down
GigabitEthernet0/2 is up, line protocol is up
```

Accessing the CLI

You can open the access point/bridge’s CLI using Telnet, Secure Shell (SSH), through the access point/bridge’s RJ-45 console port located on the power injector.

Opening the CLI with Telnet

Follow these steps to open the CLI with Telnet. These steps are for a PC running Microsoft Windows with a Telnet terminal application. Check your PC operating instructions for detailed instructions for your operating system.

-
- Step 1** Select **Start > 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 drop-down menus. To start the Telnet session in Windows 2000, type **open** followed by the access point/bridge's IP address.

- Step 3** In the Host Name field, type the access point/bridge's IP address and click **Connect**.
- Step 4** At the username and password prompts, enter your administrator username and password. The default username is **Cisco**, and the default password is **Cisco**. The default enable password is also **Cisco**. Usernames and passwords are case-sensitive.

Opening the CLI with Secure Shell

Secure Shell Protocol is a protocol that provides a secure, remote connection to networking devices set up to use it. Secure Shell (SSH) is a software package that provides secure login sessions by encrypting the entire session. SSH features strong cryptographic authentication, strong encryption, and integrity protection. For detailed information on SSH, visit the homepage of SSH Communications Security, Ltd. at this URL: <http://www.ssh.com/>

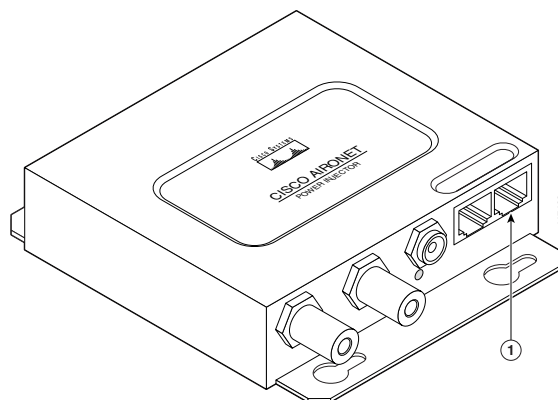
SSH provides more security for remote connections than Telnet by providing strong encryption when a device is authenticated. See the “[Configuring Client ARP Caching](#)” section on page 5-24 for detailed instructions on setting up the access point/bridge for SSH access.

Opening the CLI Using the Console Port

If you need to configure the access point/bridge locally (without connecting to a wired LAN), you can connect a PC to power injector's serial port using a DB-9 to RJ-45 serial cable. Follow these steps to open the CLI by connecting to the serial port:

- Step 1** Connect a nine-pin, female DB-9 to RJ-45 serial cable to the RJ-45 serial port on the power injector and to the COM port on your PC. [Figure 4-1](#) shows the power injector's serial port connector.

Figure 4-1 Serial Port Connector



1	Serial port connector (RJ-45 connector)

**Note**

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

- Step 2** Set up a terminal emulator to communicate with the access point/bridge. Use the following settings for the terminal emulator connection: 9600 baud, 8 data bits, no parity, 1 stop bit, and no flow control.
- Step 3** When the terminal emulator is activated, press **Enter**. An Enter Network Password window appears.
- Step 4** Enter your username in the User Name field. The default username is *Cisco*.
- Step 5** Enter the access point/bridge password in the Password field and press **Enter**. The default password is *Cisco*.

When the CLI activates, you can enter CLI commands to configure the access point/bridge.



Administering the Access Point/Bridge

This chapter describes how to administer your access point/bridge. This chapter contains these sections:

- [Preventing Unauthorized Access to Your Access Point/Bridge, page 5-2](#)
- [Protecting Access to Privileged EXEC Commands, page 5-2](#)
- [Controlling Access Point/Bridge Access with RADIUS, page 5-8](#)
- [Controlling Access Point/Bridge Access with TACACS+, page 5-13](#)
- [Configuring Ethernet Speed and Duplex Settings, page 5-16](#)
- [Configuring the Access Point/Bridge for Local Authentication and Authorization, page 5-17](#)
- [Configuring the Authentication Cache and Profile, page 5-18](#)
- [Configuring Client ARP Caching, page 5-24](#)
- [Configuring Client ARP Caching, page 5-24](#)
- [Managing the System Time and Date, page 5-26](#)
- [Configuring a System Name and Prompt, page 5-38](#)
- [Creating a Banner, page 5-41](#)

Preventing Unauthorized Access to Your Access Point/Bridge

You can prevent unauthorized users from reconfiguring your access point/bridge and viewing configuration information. Typically, you want network administrators to have access to the access point/bridge while you restrict access to users who connect through a terminal or workstation from within the local network.

To prevent unauthorized access to your access point/bridge, you should configure one of these security features:

- Username and password pairs, which are locally stored on the access point/bridge. These pairs authenticate each user before that user can access the access point/bridge. You can also assign a specific privilege level (read only or read/write) to each username and password pair. For more information, see the [“Configuring Username and Password Pairs” section on page 5-6](#).

**Note**

The default username is *Cisco*, and the default password is *Cisco*.
Usernames and passwords are case-sensitive.

- Username and password pairs stored centrally in a database on a security server. For more information, see the [“Controlling Access Point/Bridge Access with RADIUS” section on page 5-8](#).

Protecting Access to Privileged EXEC Commands

A simple way of providing terminal access control in your network is to use passwords and assign privilege levels. Password protection restricts access to a network or network device. Privilege levels define what commands users can issue after they have logged into a network device.

**Note**

For complete syntax and usage information for the commands used in this section, refer to the *Cisco IOS Security Command Reference for Release 12.2*.

This section describes how to control access to the configuration file and privileged EXEC commands. It contains this configuration information:

- [Default Password and Privilege Level Configuration, page 5-3](#)
- [Setting or Changing a Static Enable Password, page 5-3](#)
- [Protecting Enable and Enable Secret Passwords with Encryption, page 5-4](#)
- [Configuring Username and Password Pairs, page 5-6](#)
- [Configuring Multiple Privilege Levels, page 5-6](#)

Default Password and Privilege Level Configuration

Table 5-1 shows the default password and privilege level configuration.

Table 5-1 *Default Password and Privilege Levels*

Feature	Default Setting
Username and password	Default username is <i>Cisco</i> and the default password is <i>Cisco</i> .
Enable password and privilege level	Default password is <i>Cisco</i> . The default is level 15 (privileged EXEC level). The password is encrypted in the configuration file.
Enable secret password and privilege level	The default enable password is <i>Cisco</i> . The default is level 15 (privileged EXEC level). The password is encrypted before it is written to the configuration file.
Line password	Default password is <i>Cisco</i> . The password is encrypted in the configuration file.

Setting or Changing a Static Enable Password

The enable password controls access to the privileged EXEC mode.



Note

The **no enable password** global configuration command removes the enable password, but you should use extreme care when using this command. If you remove the enable password, you are locked out of the EXEC mode.

Beginning in privileged EXEC mode, follow these steps to set or change a static enable password:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	enable password <i>password</i>	Define a new password or change an existing password for access to privileged EXEC mode. The default password is <i>Cisco</i>. For <i>password</i>, specify a string from 1 to 25 alphanumeric characters. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces. It can contain the question mark (?) character if you precede the question mark with the key combination Ctrl-V when you create the password; for example, to create the password abc?123, do this: 1. Enter abc. 2. Enter Ctrl-V. 3. Enter ?123. When the system prompts you to enter the enable password, you need not precede the question mark with the Ctrl-V; you can simply enter abc?123 at the password prompt.
Step 3	end	Return to privileged EXEC mode.

	Command	Purpose
Step 4	show running-config	Verify your entries.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file. The enable password is not encrypted and can be read in the access point/bridge configuration file.

This example shows how to change the enable password to *11u2c3k4y5*. The password is not encrypted and provides access to level 15 (traditional privileged EXEC mode access):

```
bridge(config)# enable password 11u2c3k4y5
```

Protecting Enable and Enable Secret Passwords with Encryption

To provide an additional layer of security, particularly for passwords that cross the network or that are stored on a Trivial File Transfer Protocol (TFTP) server, you can use either the **enable password** or **enable secret** global configuration commands. Both commands accomplish the same thing; that is, you can establish an encrypted password that users must enter to access privileged EXEC mode (the default) or any privilege level you specify.

We recommend that you use the **enable secret** command because it uses an improved encryption algorithm.

If you configure the **enable secret** command, it takes precedence over the **enable password** command; the two commands cannot be in effect simultaneously.

Beginning in privileged EXEC mode, follow these steps to configure encryption for enable and enable secret passwords:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	enable password [level <i>level</i>] { <i>password</i> <i>encryption-type encrypted-password</i> } or enable secret [level <i>level</i>] { <i>password</i> <i>encryption-type encrypted-password</i> }	Define a new password or change an existing password for access to privileged EXEC mode. or Define a secret password, which is saved using a nonreversible encryption method. (Optional) For <i>level</i>, the range is from 0 to 15. Level 1 is normal user EXEC mode privileges. The default level is 15 (privileged EXEC mode privileges). - For <i>password</i>, specify a string from 1 to 25 alphanumeric characters. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces. By default, no password is defined. (Optional) For <i>encryption-type</i>, only type 5, a Cisco proprietary encryption algorithm, is available. If you specify an encryption type, you must provide an encrypted password—an encrypted password you copy from another access point/bridge configuration. Note If you specify an encryption type and then enter a clear text password, you can not re-enter privileged EXEC mode. You cannot recover a lost encrypted password by any method.
Step 3	service password-encryption	(Optional) Encrypt the password when the password is defined or when the configuration is written. Encryption prevents the password from being readable in the configuration file.
Step 4	end	Return to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

If both the enable and enable secret passwords are defined, users must enter the enable secret password.

Use the **level** keyword to define a password for a specific privilege level. After you specify the level and set a password, give the password only to users who need to have access at this level. Use the **privilege level** global configuration command to specify commands accessible at various levels. For more information, see the [“Configuring Multiple Privilege Levels” section on page 5-6](#).

If you enable password encryption, it applies to all passwords including username passwords, authentication key passwords, the privileged command password, and console and virtual terminal line passwords.

To remove a password and level, use the **no enable password** [level *level*] or **no enable secret** [level *level*] global configuration command. To disable password encryption, use the **no service password-encryption** global configuration command.

This example shows how to configure the encrypted password *\$1\$FaD0\$Xyti5Rkls3LoyxzS8* for privilege level 2:

```
ap(config)# enable secret level 2 5 $1$FaD0$Xyti5Rkls3LoyxzS8
```

Configuring Username and Password Pairs

You can configure username and password pairs, which are locally stored on the access point/bridge. These pairs are assigned to lines or interfaces and authenticate each user before that user can access the access point/bridge. If you have defined privilege levels, you can also assign a specific privilege level (with associated rights and privileges) to each username and password pair.

Beginning in privileged EXEC mode, follow these steps to establish a username-based authentication system that requests a login username and a password:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	username <i>name</i> [privilege <i>level</i>] { password <i>encryption-type password</i> }	Enter the username, privilege level, and password for each user. - For <i>name</i>, specify the user ID as one word. Spaces and quotation marks are not allowed. (Optional) For <i>level</i>, specify the privilege level the user has after gaining access. The range is 0 to 15. Level 15 gives privileged EXEC mode access. Level 1 gives user EXEC mode access. - For <i>encryption-type</i>, enter 0 to specify that an unencrypted password will follow. Enter 7 to specify that a hidden password will follow. - For <i>password</i>, specify the password the user must enter to gain access to the access point/bridge. The password must be from 1 to 25 characters, can contain embedded spaces, and must be the last option specified in the username command.
Step 3	login local	Enable local password checking at login time. Authentication is based on the username specified in Step 2.
Step 4	end	Return to privileged EXEC mode.
Step 5	show running-config	Verify your entries.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To disable username authentication for a specific user, use the **no username** *name* global configuration command.

To disable password checking and allow connections without a password, use the **no login** line configuration command.



Note

You must have at least one username configured and you must have login local set to open a Telnet session to the access point/bridge. If you enter no username for the only username, you can be locked out of the access point/bridge.

Configuring Multiple Privilege Levels

By default, Cisco IOS software has two modes of password security: user EXEC and privileged EXEC. You can configure up to 16 hierarchical levels of commands for each mode. By configuring multiple passwords, you can allow different sets of users to have access to specified commands.

For example, if you want many users to have access to the **clear line** command, you can assign it level 2 security and distribute the level 2 password fairly widely. But if you want more restricted access to the **configure** command, you can assign it level 3 security and distribute that password to a more restricted group of users.

This section includes this configuration information:

- [Setting the Privilege Level for a Command, page 5-7](#)
- [Logging Into and Exiting a Privilege Level, page 5-8](#)

Setting the Privilege Level for a Command

Beginning in privileged EXEC mode, follow these steps to set the privilege level for a command mode:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	privilege mode level level command	Set the privilege level for a command. • For <i>mode</i>, enter configure for global configuration mode, exec for EXEC mode, interface for interface configuration mode, or line for line configuration mode. • For <i>level</i>, the range is from 0 to 15. Level 1 is for normal user EXEC mode privileges. Level 15 is the level of access permitted by the enable password. • For <i>command</i>, specify the command to which you want to restrict access.
Step 3	enable password level level password	Specify the enable password for the privilege level. • For <i>level</i>, the range is from 0 to 15. Level 1 is for normal user EXEC mode privileges. • For <i>password</i>, specify a string from 1 to 25 alphanumeric characters. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces. By default, no password is defined.
Step 4	end	Return to privileged EXEC mode.
Step 5	show running-config or show privilege	Verify your entries. The first command displays the password and access level configuration. The second command displays the privilege level configuration.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

When you set a command to a privilege level, all commands whose syntax is a subset of that command are also set to that level. For example, if you set the **show ip route** command to level 15, the **show** commands and **show ip** commands are automatically set to privilege level 15 unless you set them individually to different levels.

To return to the default privilege for a given command, use the **no privilege mode level level command** global configuration command.

This example shows how to set the **configure** command to privilege level 14 and define *SecretPswd14* as the password users must enter to use level 14 commands:

```
ap(config)# privilege exec level 14 configure
ap(config)# enable password level 14 SecretPswd14
```

Logging Into and Exiting a Privilege Level

Beginning in privileged EXEC mode, follow these steps to log in to a specified privilege level and to exit to a specified privilege level:

	Command	Purpose
Step 1	enable <i>level</i>	Log in to a specified privilege level. For <i>level</i> , the range is 0 to 15.
Step 2	disable <i>level</i>	Exit to a specified privilege level. For <i>level</i> , the range is 0 to 15.

Controlling Access Point/Bridge Access with RADIUS

This section describes how to control administrator access to the access point/bridge using Remote Authentication Dial-In User Service (RADIUS). For complete instructions on configuring the access point/bridge to support RADIUS, see [Chapter 12, “Configuring RADIUS and TACACS+ Servers.”](#)

RADIUS provides detailed accounting information and flexible administrative control over authentication and authorization processes. RADIUS is facilitated through AAA and can be enabled only through AAA commands.



Note

For complete syntax and usage information for the commands used in this section, refer to the *Cisco IOS Security Command Reference for Release 12.2*.

These sections describe RADIUS configuration:

- [Default RADIUS Configuration, page 5-8](#)
- [Configuring RADIUS Login Authentication, page 5-9](#) (required)
- [Defining AAA Server Groups, page 5-10](#) (optional)
- [Configuring RADIUS Authorization for User Privileged Access and Network Services, page 5-12](#) (optional)
- [Displaying the RADIUS Configuration, page 5-13](#)

Default RADIUS Configuration

RADIUS and AAA are disabled by default.

To prevent a lapse in security, you cannot configure RADIUS through a network management application. When enabled, RADIUS can authenticate users accessing the access point/bridge through the CLI.

Configuring RADIUS Login Authentication

To configure AAA authentication, you define a named list of authentication methods and then apply that list to various interfaces. The method list defines the types of authentication to be performed and the sequence in which they are performed; it must be applied to a specific interface before any of the defined authentication methods are performed. The only exception is the default method list (which, by coincidence, is named *default*). The default method list is automatically applied to all interfaces except those that have a named method list explicitly defined.

A method list describes the sequence and authentication methods to be queried to authenticate a user. You can designate one or more security protocols to be used for authentication, thus ensuring a backup system for authentication in case the initial method fails. The software uses the first method listed to authenticate users; if that method fails to respond, the software selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this cycle—meaning that the security server or local username database responds by denying the user access—the authentication process stops, and no other authentication methods are attempted.

Beginning in privileged EXEC mode, follow these steps to configure login authentication. This procedure is required.

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	aaa new-model	Enable AAA.
Step 3	aaa authentication login { default list-name } method1 [method2...]	Create a login authentication method list. - To create a default list that is used when a named list is <i>not</i> specified in the login authentication command, use the default keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all interfaces. - For <i>list-name</i>, specify a character string to name the list you are creating. - For <i>method1...</i>, specify the actual method the authentication algorithm tries. The additional methods of authentication are used only if the previous method returns an error, not if it fails. Select one of these methods: local—Use the local username database for authentication. You must enter username information in the database. Use the username password global configuration command. radius—Use RADIUS authentication. You must configure the RADIUS server before you can use this authentication method. For more information, see the “Identifying the RADIUS Server Host” section on page 12-5.
Step 4	line [console tty vty] line-number [ending-line-number]	Enter line configuration mode, and configure the lines to which you want to apply the authentication list.

	Command	Purpose
Step 5	login authentication { default <i>list-name</i> }	Apply the authentication list to a line or set of lines. - If you specify default, use the default list created with the aaa authentication login command. - For <i>list-name</i>, specify the list created with the aaa authentication login command.
Step 6	end	Return to privileged EXEC mode.
Step 7	show running-config	Verify your entries.
Step 8	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To disable AAA, use the **no aaa new-model** global configuration command. To disable AAA authentication, use the **no aaa authentication login** { **default** | *list-name* } *method1* [*method2*...] global configuration command. To either disable RADIUS authentication for logins or to return to the default value, use the **no login authentication** { **default** | *list-name* } line configuration command.

Defining AAA Server Groups

You can configure the access point/bridge to use AAA server groups to group existing server hosts for authentication. You select a subset of the configured server hosts and use them for a particular service. The server group is used with a global server-host list, which lists the IP addresses of the selected server hosts.

Server groups also can include multiple host entries for the same server if each entry has a unique identifier (the combination of the IP address and UDP port number), allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. If you configure two different host entries on the same RADIUS server for the same service (such as accounting), the second configured host entry acts as a fail-over backup to the first one.

You use the **server** group server configuration command to associate a particular server with a defined group server. You can either identify the server by its IP address or identify multiple host instances or entries by using the optional **auth-port** and **acct-port** keywords.

Beginning in privileged EXEC mode, follow these steps to define the AAA server group and associate a particular RADIUS server with it:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	aaa new-model	Enable AAA.

	Command	Purpose
Step 3	radius-server host { <i>hostname</i> <i>ip-address</i> } [auth-port <i>port-number</i>] [acct-port <i>port-number</i>] [timeout <i>seconds</i>] [retransmit <i>retries</i>] [key <i>string</i>]	Specify the IP address or host name of the remote RADIUS server host. (Optional) For auth-port <i>port-number</i>, specify the UDP destination port for authentication requests. (Optional) For acct-port <i>port-number</i>, specify the UDP destination port for accounting requests. (Optional) For timeout <i>seconds</i>, specify the time interval that the access point/bridge waits for the RADIUS server to reply before retransmitting. The range is 1 to 1000. This setting overrides the radius-server timeout global configuration command setting. If no timeout is set with the radius-server host command, the setting of the radius-server timeout command is used. (Optional) For retransmit <i>retries</i>, specify the number of times a RADIUS request is resent to a server if that server is not responding or responding slowly. The range is 1 to 1000. If no retransmit value is set with the radius-server host command, the setting of the radius-server retransmit global configuration command is used. (Optional) For key <i>string</i>, specify the authentication and encryption key used between the access point/bridge and the RADIUS daemon running on the RADIUS server. Note The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the radius-server host command. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key. To configure the access point/bridge to recognize more than one host entry associated with a single IP address, enter this command as many times as necessary, making sure that each UDP port number is different. The access point/bridge software searches for hosts in the order in which you specify them. Set the timeout, retransmit, and encryption key values to use with the specific RADIUS host.
Step 4	aaa group server radius <i>group-name</i>	Define the AAA server-group with a group name. This command puts the access point/bridge in a server group configuration mode.
Step 5	server <i>ip-address</i>	Associate a particular RADIUS server with the defined server group. Repeat this step for each RADIUS server in the AAA server group. Each server in the group must be previously defined in Step 2.
Step 6	end	Return to privileged EXEC mode.
Step 7	show running-config	Verify your entries.
Step 8	copy running-config startup-config	(Optional) Save your entries in the configuration file.
Step 9		Enable RADIUS login authentication. See the “Configuring RADIUS Login Authentication” section on page 5-9.

To remove the specified RADIUS server, use the **no radius-server host** *hostname* | *ip-address* global configuration command. To remove a server group from the configuration list, use the **no aaa group server radius** *group-name* global configuration command. To remove the IP address of a RADIUS server, use the **no server** *ip-address* server group configuration command.

In this example, the access point/bridge is configured to recognize two different RADIUS group servers (*group1* and *group2*). Group1 has two different host entries on the same RADIUS server configured for the same services. The second host entry acts as a fail-over backup to the first entry.

```
apap(config)# aaa new-model
ap(config)# radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
ap(config)# radius-server host 172.10.0.1 auth-port 1645 acct-port 1646
ap(config)# aaa group server radius group1
ap(config-sg-radius)# server 172.20.0.1 auth-port 1000 acct-port 1001
ap(config-sg-radius)# exit
ap(config)# aaa group server radius group2
ap(config-sg-radius)# server 172.20.0.1 auth-port 2000 acct-port 2001
ap(config-sg-radius)# exit
```

Configuring RADIUS Authorization for User Privileged Access and Network Services

AAA authorization limits the services available to a user. When AAA authorization is enabled, the access point/bridge uses information retrieved from the user's profile, which is in the local user database or on the security server, to configure the user's session. The user is granted access to a requested service only if the information in the user profile allows it.

You can use the **aaa authorization** global configuration command with the **radius** keyword to set parameters that restrict a user's network access to privileged EXEC mode.

The **aaa authorization exec radius local** command sets these authorization parameters:

- Use RADIUS for privileged EXEC access authorization if authentication was performed by using RADIUS.
- Use the local database if authentication was not performed by using RADIUS.



Note

Authorization is bypassed for authenticated users who log in through the CLI even if authorization has been configured.

Beginning in privileged EXEC mode, follow these steps to specify RADIUS authorization for privileged EXEC access and network services:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	aaa authorization network radius	Configure the access point/bridge for user RADIUS authorization for all network-related service requests.
Step 3	aaa authorization exec radius	Configure the access point/bridge for user RADIUS authorization to determine if the user has privileged EXEC access. The exec keyword might return user profile information (such as autocommand information).
Step 4	end	Return to privileged EXEC mode.
Step 5	show running-config	Verify your entries.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To disable authorization, use the **no aaa authorization {network | exec} method1** global configuration command.

Displaying the RADIUS Configuration

To display the RADIUS configuration, use the **show running-config** privileged EXEC command.

Controlling Access Point/Bridge Access with TACACS+

This section describes how to control administrator access to the access point/bridge using Terminal Access Controller Access Control System Plus (TACACS+). For complete instructions on configuring the access point/bridge to support TACACS+, see [Chapter 12, “Configuring RADIUS and TACACS+ Servers.”](#)

TACACS+ provides detailed accounting information and flexible administrative control over authentication and authorization processes. TACACS+ is facilitated through AAA and can be enabled only through AAA commands.



Note

For complete syntax and usage information for the commands used in this section, refer to the *Cisco IOS Security Command Reference for Release 12.2*.

These sections describe TACACS+ configuration:

- [Default TACACS+ Configuration, page 5-14](#)
- [Configuring TACACS+ Login Authentication, page 5-14](#)
- [Configuring TACACS+ Authorization for Privileged EXEC Access and Network Services, page 5-15](#)
- [Displaying the TACACS+ Configuration, page 5-16](#)

Default TACACS+ Configuration

TACACS+ and AAA are disabled by default.

To prevent a lapse in security, you cannot configure TACACS+ through a network management application. When enabled, TACACS+ can authenticate administrators accessing the access point/bridge through the CLI.

Configuring TACACS+ Login Authentication

To configure AAA authentication, you define a named list of authentication methods and then apply that list to various interfaces. The method list defines the types of authentication to be performed and the sequence in which they are performed; it must be applied to a specific interface before any of the defined authentication methods are performed. The only exception is the default method list (which, by coincidence, is named *default*). The default method list is automatically applied to all interfaces except those that have a named method list explicitly defined. A defined method list overrides the default method list.

A method list describes the sequence and authentication methods to be queried to authenticate a user. You can designate one or more security protocols to be used for authentication, thus ensuring a backup system for authentication in case the initial method fails. The software uses the first method listed to authenticate users; if that method fails, the software selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this cycle—meaning that the security server or local username database responds by denying the user access—the authentication process stops, and no other authentication methods are attempted.

Beginning in privileged EXEC mode, follow these steps to configure login authentication. This procedure is required.

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	aaa new-model	Enable AAA.

	Command	Purpose
Step 3	aaa authentication login { default <i>list-name</i> } <i>method1</i> [<i>method2...</i>]	Create a login authentication method list. - To create a default list that is used when a named list is <i>not</i> specified in the login authentication command, use the default keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all interfaces. - For <i>list-name</i>, specify a character string to name the list you are creating. - For <i>method1...</i>, specify the actual method the authentication algorithm tries. The additional methods of authentication are used only if the previous method returns an error, not if it fails. Select one of these methods: local—Use the local username database for authentication. You must enter username information into the database. Use the username password global configuration command. tacacs+—Use TACACS+ authentication. You must configure the TACACS+ server before you can use this authentication method.
Step 4	line [console tty vty] <i>line-number</i> [<i>ending-line-number</i>]	Enter line configuration mode, and configure the lines to which you want to apply the authentication list.
Step 5	login authentication { default <i>list-name</i> }	Apply the authentication list to a line or set of lines. - If you specify default, use the default list created with the aaa authentication login command. - For <i>list-name</i>, specify the list created with the aaa authentication login command.
Step 6	end	Return to privileged EXEC mode.
Step 7	show running-config	Verify your entries.
Step 8	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To disable AAA, use the **no aaa new-model** global configuration command. To disable AAA authentication, use the **no aaa authentication login** { **default** | *list-name* } *method1* [*method2...*] global configuration command. To either disable TACACS+ authentication for logins or to return to the default value, use the **no login authentication** { **default** | *list-name* } line configuration command.

Configuring TACACS+ Authorization for Privileged EXEC Access and Network Services

AAA authorization limits the services available to a user. When AAA authorization is enabled, the access point/bridge uses information retrieved from the user's profile, which is located either in the local user database or on the security server, to configure the user's session. The user is granted access to a requested service only if the information in the user profile allows it.

You can use the **aaa authorization** global configuration command with the **tacacs+** keyword to set parameters that restrict a user's network access to privileged EXEC mode.

The **aaa authorization exec tacacs+ local** command sets these authorization parameters:

- Use TACACS+ for privileged EXEC access authorization if authentication was performed by using TACACS+.
- Use the local database if authentication was not performed by using TACACS+.



Note

Authorization is bypassed for authenticated users who log in through the CLI even if authorization has been configured.

Beginning in privileged EXEC mode, follow these steps to specify TACACS+ authorization for privileged EXEC access and network services:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	aaa authorization network tacacs+	Configure the access point/bridge for user TACACS+ authorization for all network-related service requests.
Step 3	aaa authorization exec tacacs+	Configure the access point/bridge for user TACACS+ authorization to determine if the user has privileged EXEC access. The exec keyword might return user profile information (such as autocommand information).
Step 4	end	Return to privileged EXEC mode.
Step 5	show running-config	Verify your entries.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To disable authorization, use the **no aaa authorization {network | exec} method1** global configuration command.

Displaying the TACACS+ Configuration

To display TACACS+ server statistics, use the **show tacacs** privileged EXEC command.

Configuring Ethernet Speed and Duplex Settings

The access point/bridge power injector contains an embedded 10/100baseT switch, which is unconfigurable. The ports on the switch are set for auto-speed and auto-duplex, and auto-MDIX. Port 0 on the switch is used for the coaxial link to the bridge; port 1 on the switch is used for the RJ-45 jack on the power injector. The other switch ports are unused.

The speed and duplex settings on the bridge FastEthernet0 interface only apply to the link between the bridge port and port 0 in the power injector switch. They are entirely independent of the speed/duplex used on the RJ-45 port on the power injector. Therefore, for best performance, the bridge FastEthernet must always be set to auto speed and auto duplex. This setting results in 100 Mbps, full duplex used on the link between the bridge and power injector.

The Fast Ethernet Settings page contains the following caution:



Caution

Do not modify the 'Requested Duplex' or 'Requested Speed' while using inline power. Changing these settings while using inline power may cause the device to reboot. See documentation for details.

The following guidelines for setting Ethernet speed and duplex should always be observed:

- The internal FastEthernet0 interface should always be set for speed auto and duplex auto regardless of the settings of the device to which the external LAN port on the power injector is connected (the connecting port).
- The connecting port should always be set for one of the following:
 - 100 Mbps, auto duplex (recommended)
 - 100 Mbps, half duplex
 - 10 Mbps, auto duplex
 - 10 Mbps, half duplex



Note

Setting the port to 10 Mbps will most likely degrade throughput.

- The connecting port should never be set to full duplex.

Failure to follow these guidelines will result in lost data due to late collisions, CRC errors, etc.

Configuring the Access Point/Bridge for Local Authentication and Authorization

You can configure AAA to operate without a server by setting the access point/bridge to implement AAA in local mode. The access point/bridge then handles authentication and authorization. No accounting is available in this configuration.

Beginning in privileged EXEC mode, follow these steps to configure the access point/bridge for local AAA:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	aaa new-model	Enable AAA.
Step 3	aaa authentication login default local	Set the login authentication to use the local username database. The default keyword applies the local user database authentication to all interfaces.
Step 4	aaa authorization exec local	Configure user AAA authorization to determine if the user is allowed to run an EXEC shell by checking the local database.
Step 5	aaa authorization network local	Configure user AAA authorization for all network-related service requests.

	Command	Purpose
Step 6	username <i>name</i> [privilege <i>level</i>] { password <i>encryption-type</i> <i>password</i> }	Enter the local database, and establish a username-based authentication system. Repeat this command for each user. - For <i>name</i>, specify the user ID as one word. Spaces and quotation marks are not allowed. (Optional) For <i>level</i>, specify the privilege level the user has after gaining access. The range is 0 to 15. Level 15 gives privileged EXEC mode access. Level 0 gives user EXEC mode access. - For <i>encryption-type</i>, enter 0 to specify that an unencrypted password follows. Enter 7 to specify that a hidden password follows. - For <i>password</i>, specify the password the user must enter to gain access to the access point/bridge. The password must be from 1 to 25 characters, can contain embedded spaces, and must be the last option specified in the username command.
Step 7	end	Return to privileged EXEC mode.
Step 8	show running-config	Verify your entries.
Step 9	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To disable AAA, use the **no aaa new-model** global configuration command. To disable authorization, use the **no aaa authorization** {**network** | **exec**} *method1* global configuration command.

Configuring the Authentication Cache and Profile

The authentication cache and profile feature allows the access point/bridge to cache the authentication/authorization responses for a user so that subsequent authentication/authorization requests do not need to be sent to the AAA server.



Note

On the access point/bridge, this feature is only supported for Admin authentication.

The following commands that support this feature are included in Release 12.3(7):

```
cache expiry
cache authorization profile
cache authentication profile
aaa cache profile
```



Note

See the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges, 12.3(7)JA* for information about these commands.

The following is an example configuration from an access point configured for Admin authentication using TACACS+ with the auth cache enabled. While this example is based on a TACACS server, the access point could be configured for Admin authentication using RADIUS:

```
version 12.3
no service pad
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
service password-encryption
!
hostname ap
!
!
username Cisco password 7 123A0C041104
username admin privilege 15 password 7 01030717481C091D25
ip subnet-zero
!
!
aaa new-model
!
!
aaa group server radius rad_eap
server 192.168.134.229 auth-port 1645 acct-port 1646
!
aaa group server radius rad_mac
server 192.168.134.229 auth-port 1645 acct-port 1646
!
aaa group server radius rad_acct
server 192.168.134.229 auth-port 1645 acct-port 1646
!
aaa group server radius rad_admin
server 192.168.134.229 auth-port 1645 acct-port 1646
cache expiry 1
cache authorization profile admin_cache
cache authentication profile admin_cache
!
aaa group server tacacs+ tac_admin
server 192.168.133.231
cache expiry 1
cache authorization profile admin_cache
cache authentication profile admin_cache
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa authentication login default local cache tac_admin group tac_admin
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authorization exec default local cache tac_admin group tac_admin
aaa accounting network acct_methods start-stop group rad_acct
aaa cache profile admin_cache
all
!
aaa session-id common
!
!
!
!
bridge irb
!
!
interface Dot11Radio0
no ip address
no ip route-cache
shutdown
speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
```

```

no bridge-group 1 unicast-flooding
bridge-group 1 spanning-disabled
!
interface Dot11Radio1
no ip address
no ip route-cache
shutdown
speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
bridge-group 1 spanning-disabled
!
interface FastEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
bridge-group 1
no bridge-group 1 source-learning
bridge-group 1 spanning-disabled
!
interface BVI1
ip address 192.168.133.207 255.255.255.0
no ip route-cache
!
ip http server
ip http authentication aaa
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
!
tacacs-server host 192.168.133.231 key 7 105E080A16001D1908
tacacs-server directed-request
radius-server attribute 32 include-in-access-req format %h
radius-server host 192.168.134.229 auth-port 1645 acct-port 1646 key 7 111918160405041E00
radius-server vsa send accounting
!
control-plane
!
bridge 1 route ip
!
!
!
line con 0
transport preferred all
transport output all
line vty 0 4
transport preferred all
transport input all
transport output all
line vty 5 15
transport preferred all
transport input all
transport output all
!
end

```


Configuring the Access Point/Bridge to Provide DHCP Service

These sections describe how to configure the access point/bridge to act as a DHCP server:

- [Setting up the DHCP Server, page 5-21](#)
- [Monitoring and Maintaining the DHCP Server Access Point, page 5-22](#)

Setting up the DHCP Server

By default, access points are configured to receive IP settings from a DHCP server on your network. You can also configure an access point to act as a DHCP server to assign IP settings to devices on both your wired and wireless LANs.

When configured as an access point, the access point/bridge becomes a mini-DHCP server by default when it is configured with factory default settings and it cannot receive IP settings from a DHCP server. As a mini-DHCP server, the access point/bridge provides up to 20 IP addresses between 10.0.0.11 and 10.0.0.30 to a PC connected to its Ethernet port and to wireless client devices configured to use either no SSID or *tsunami* as the SSID, and with all security settings disabled. The mini-DHCP server feature is disabled automatically when you assign a static IP address to the access point/bridge.



Note

When you configure the access point/bridge as a DHCP server, it assigns IP addresses to devices on its subnet. The devices communicate with other devices on the subnet but not beyond it. If data needs to be passed beyond the subnet, you must assign a default router. The IP address of the default router should be on the same subnet as the access point configured as the DHCP server.

For detailed information on DHCP-related commands and options, refer to the Configuring DHCP chapter in the *Cisco IOS IP Configuration Guide, Release 12.3*. Click this URL to browse to the “Configuring DHCP” chapter:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcprt1/1cfdhcp.htm

Beginning in privileged EXEC mode, follow these steps to configure an access point to provide DHCP service:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	ip dhcp excluded-address <i>low_address</i> [<i>high_address</i>]	Exclude the access point/bridge's IP address from the range of addresses the wireless device assigns. Enter the IP address in four groups of characters, such as 10.91.6.158. the access point/bridge assumes that all IP addresses in a DHCP address pool subnet are available for assigning to DHCP clients. You must specify the IP addresses that the DHCP Server should not assign to clients. (Optional) To enter a range of excluded addresses, enter the address at the low end of the range followed by the address at the high end of the range.
Step 3	ip dhcp pool <i>pool_name</i>	Create a name for the pool of IP addresses that the wireless device assigns in response to DHCP requests, and enter DHCP configuration mode.

	Command	Purpose
Step 4	network <i>subnet_number</i> [<i>mask</i> <i>prefix-length</i>]	Assign the subnet number for the address pool. The access point/bridge assigns IP addresses within this subnet. (Optional) Assign a subnet mask for the address pool, or specify the number of bits that comprise the address prefix. The prefix is an alternative way of assigning the network mask. The prefix length must be preceded by a forward slash (/).
Step 5	lease { <i>days</i> [<i>hours</i>] [<i>minutes</i>] infinite }	Configure the duration of the lease for IP addresses assigned by the wireless device. • <i>days</i>—configure the lease duration in number of days • (optional) <i>hours</i>—configure the lease duration in number of hours • (optional) <i>minutes</i>—configure the lease duration in number of minutes • infinite—set the lease duration to infinite
Step 6	default-router <i>address</i> [<i>address2</i> ... <i>address8</i>]	Specify the IP address of the default router for DHCP clients on the subnet. One IP address is required, however, you can specify up to eight addresses in one command line.
Step 7	end	Return to privileged EXEC mode.
Step 8	show running-config	Verify your entries.
Step 9	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Use the **no** form of these commands to return to default settings.

This example shows how to configure the wireless device as a DHCP server, exclude a range of IP address, and assign a default router:

```
AP# configure terminal
AP(config)# ip dhcp excluded-address 172.16.1.1 172.16.1.20
AP(config)# ip dhcp pool wishbone
AP(dhcp-config)# network 172.16.1.0 255.255.255.0
AP(dhcp-config)# lease 10
AP(dhcp-config)# default-router 172.16.1.1
AP(dhcp-config)# end
```

Monitoring and Maintaining the DHCP Server Access Point

These sections describe commands you can use to monitor and maintain the DHCP server access point:

- [Show Commands, page 5-22](#)
- [Clear Commands, page 5-23](#)
- [Debug Command, page 5-23](#)

Show Commands

In Exec mode, enter the commands in [Table 5-2](#) to display information about the access point/bridge as DHCP server.

Table 5-2 Show Commands for DHCP Server

Command	Purpose
show ip dhcp conflict [<i>address</i>]	Displays a list of all address conflicts recorded by a specific DHCP server. Enter the access point/bridge's IP address to show conflicts recorded by the access point/bridge.
show ip dhcp database [<i>url</i>]	Displays recent activity on the DHCP database. Note Use this command in privileged EXEC mode.
show ip dhcp server statistics	Displays count information about server statistics and messages sent and received.

Clear Commands

In privileged Exec mode, use the commands in [Table 5-3](#) to clear DHCP server variables.

Table 5-3 Clear Commands for DHCP Server

Command	Purpose
clear ip dhcp binding { <i>address</i> * }	Deletes an automatic address binding from the DHCP database. Specifying the address argument clears the automatic binding for a specific (client) IP address. Specifying an asterisk (*) clears all automatic bindings.
clear ip dhcp conflict { <i>address</i> * }	Clears an address conflict from the DHCP database. Specifying the address argument clears the conflict for a specific IP address. Specifying an asterisk (*) clears conflicts for all addresses.
clear ip dhcp server statistics	Resets all DHCP server counters to 0.

Debug Command

To enable DHCP server debugging, use this command in privileged EXEC mode:

debug ip dhcp server { *events* | *packets* | *linkage* }

Use the **no** form of the command to disable debugging for the wireless device DHCP server.

Configuring the Access Point for Secure Shell

This section describes how to configure the Secure Shell (SSH) feature.



Note

For complete syntax and usage information for the commands used in this section, refer to the “Secure Shell Commands” section in the *Cisco IOS Security Command Reference for Release 12.3*.

Understanding SSH

SSH is a protocol that provides a secure, remote connection to a Layer 2 or a Layer 3 device. There are two versions of SSH: SSH version 1 and SSH version 2. This software release supports both SSH versions. If you do not specify the version number, the access point defaults to version 2.

SSH provides more security for remote connections than Telnet by providing strong encryption when a device is authenticated. The SSH feature has an SSH server and an SSH integrated client. The client supports these user authentication methods:

- RADIUS (for more information, see the [“Controlling Access Point/Bridge Access with RADIUS” section on page 5-8](#))
- Local authentication and authorization (for more information, see the [“Configuring the Access Point/Bridge for Local Authentication and Authorization” section on page 5-17](#))

For more information about SSH, refer to Part 5, “Other Security Features” in the *Cisco IOS Security Configuration Guide for Release 12.3*.

**Note**

The SSH feature in this software release does not support IP Security (IPSec).

Configuring SSH

Before configuring SSH, download the crypto software image from Cisco.com. For more information, refer to the release notes for this release.

For information about configuring SSH and displaying SSH settings, refer to Part 5, “Other Security Features” in the *Cisco IOS Security Configuration Guide for Release 12.3*, which is available on Cisco.com at the following link:

http://cisco.com/en/US/products/sw/iosswrel/ps5187/products_installation_and_configuration_guides_list.html

Configuring Client ARP Caching

You can configure the access point/bridge to maintain an ARP cache for associated client devices. Maintaining an ARP cache on the access point/bridge reduces the traffic load on your wireless LAN. ARP caching is disabled by default.

This section contains this information:

- [Understanding Client ARP Caching, page 5-24](#)
- [Configuring ARP Caching, page 5-25](#)

Understanding Client ARP Caching

ARP caching on the access point/bridge reduces the traffic on your wireless LAN by stopping ARP requests for client devices at the wireless device. Instead of forwarding ARP requests to client devices, the access point/bridge responds to requests on behalf of associated client devices.

When ARP caching is disabled, the access point/bridge forwards all ARP requests through the radio port to associated clients, and the client to which the ARP request is directed responds. When ARP caching is enabled, the access point/bridge responds to ARP requests for associated clients and does not forward requests to clients. When the access point/bridge receives an ARP request for an IP address not in the cache, the access point/bridge drops the request and does not forward it. In its beacon, the access point/bridge includes an information element to alert client devices that they can safely ignore broadcast messages to increase battery life.

Optional ARP Caching

When a non-Cisco client device is associated to an access point and is not passing data, the access point/bridge might not know the client's IP address. If this situation occurs frequently on your wireless LAN, you can enable optional ARP caching. When ARP caching is optional, the access point/bridge responds on behalf of clients with IP addresses known to the access point/bridge but forwards out its radio port any ARP requests addressed to unknown clients. When the access point/bridge learns the IP addresses for all associated clients, it drops ARP requests not directed to its associated clients.

Configuring ARP Caching

Beginning in privileged EXEC mode, follow these steps to configure the access point/bridge to maintain an ARP cache for associated clients:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	dot11 arp-cache [optional]	Enable ARP caching on the wireless device. (Optional) Use the optional keyword to enable ARP caching only for the client devices whose IP addresses are known to the access point/bridge.
Step 3	end	Return to privileged EXEC mode.
Step 4	show running-config	Verify your entries.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to configure ARP caching on an access point:

```
ap# configure terminal
ap(config)# dot11 arp-cache
ap(config)# end
```

Managing the System Time and Date

You can manage the system time and date on your access point/bridge automatically, using the Network Time Protocol (NTP), or manually, by setting the time and date on the access point/bridge.

**Note**

For complete syntax and usage information for the commands used in this section, refer to the *Cisco IOS Configuration Fundamentals Command Reference for Release 12.2*.

This section contains this configuration information:

- [Understanding the System Clock, page 5-26](#)
- [Understanding Network Time Protocol, page 5-26](#)
- [Configuring NTP, page 5-28](#)
- [Configuring Time and Date Manually, page 5-35](#)

Understanding the System Clock

The heart of the time service is the system clock. This clock runs from the moment the system starts up and keeps track of the date and time.

The system clock can then be set from these sources:

- Network Time Protocol
- Manual configuration

The system clock can provide time to these services:

- User **show** commands
- Logging and debugging messages

The system clock determines time internally based on Universal Time Coordinated (UTC), also known as Greenwich Mean Time (GMT). You can configure information about the local time zone and summer time (daylight saving time) so that the time is correctly displayed for the local time zone.

The system clock keeps track of whether the time is *authoritative* or not (that is, whether it has been set by a time source considered to be authoritative). If it is not authoritative, the time is available only for display purposes and is not redistributed. For configuration information, see the “[Configuring Time and Date Manually](#)” section on page 5-35.

Understanding Network Time Protocol

The NTP is designed to time-synchronize a network of devices. NTP runs over User Datagram Protocol (UDP), which runs over IP. NTP is documented in RFC 1305.

An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two devices to within a millisecond of one another.

NTP uses the concept of a *stratum* to describe how many NTP hops away a device is from an authoritative time source. A stratum 1 time server has a radio or atomic clock directly attached, a stratum 2 time server receives its time through NTP from a stratum 1 time server, and so on. A device

running NTP automatically chooses as its time source the device with the lowest stratum number with which it communicates through NTP. This strategy effectively builds a self-organizing tree of NTP speakers.

NTP avoids synchronizing to a device whose time might not be accurate by never synchronizing to a device that is not synchronized. NTP also compares the time reported by several devices and does not synchronize to a device whose time is significantly different than the others, even if its stratum is lower.

The communications between devices running NTP (known as *associations*) are usually statically configured; each device is given the IP address of all devices with which it should form associations. Accurate timekeeping is possible by exchanging NTP messages between each pair of devices with an association. However, in a LAN environment, NTP can be configured to use IP broadcast messages instead. This alternative reduces configuration complexity because each device can simply be configured to send or receive broadcast messages. However, in that case, information flow is one-way only.

The time kept on a device is a critical resource; you should use the security features of NTP to avoid the accidental or malicious setting of an incorrect time. Two mechanisms are available: an access-list-based restriction scheme and an encrypted authentication mechanism.

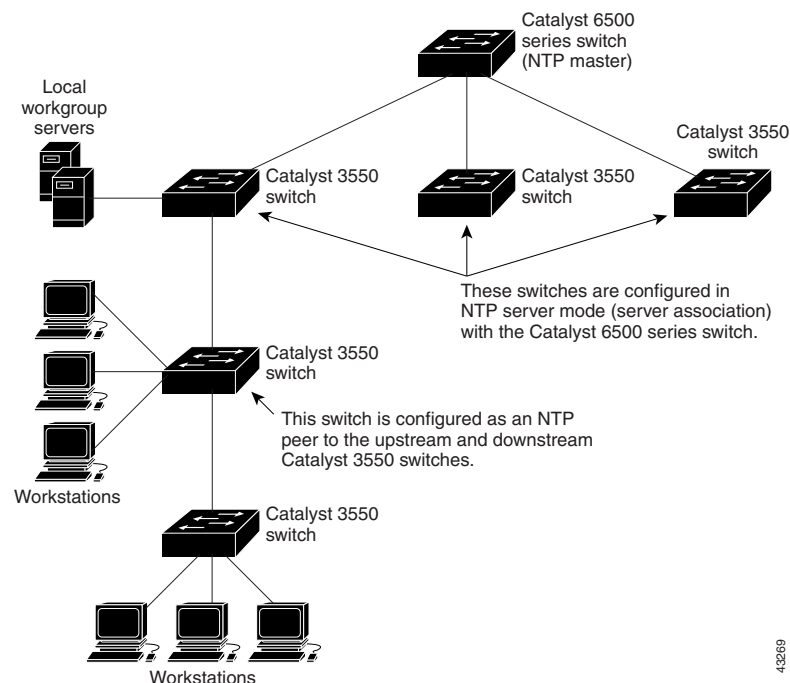
Cisco's implementation of NTP does not support stratum 1 service; it is not possible to connect to a radio or atomic clock. We recommend that the time service for your network be derived from the public NTP servers available on the IP Internet. [Figure 5-1](#) shows a typical network example using NTP.

If the network is isolated from the Internet, Cisco's implementation of NTP allows a device to act as though it is synchronized through NTP, when in fact it has determined the time by using other means. Other devices then synchronize to that device through NTP.

When multiple sources of time are available, NTP is always considered to be more authoritative. NTP time overrides the time set by any other method.

Several manufacturers include NTP software for their host systems, and a publicly available version for systems running UNIX and its various derivatives is also available. This software allows host systems to be time-synchronized as well.

Figure 5-1 Typical NTP Network Configuration



Configuring NTP

Cisco Aironet 1300 Series Access Point/Bridges do not have a hardware-supported clock, and they cannot function as an NTP master clock to which peers synchronize themselves when an external NTP source is not available. These access point/bridges also have no hardware support for a calendar. As a result, the **ntp update-calendar** and the **ntp master** global configuration commands are not available.

This section contains this configuration information:

- [Default NTP Configuration, page 5-28](#)
- [Configuring NTP Authentication, page 5-28](#)
- [Configuring NTP Associations, page 5-30](#)
- [Configuring NTP Broadcast Service, page 5-31](#)
- [Configuring NTP Access Restrictions, page 5-32](#)
- [Configuring the Source IP Address for NTP Packets, page 5-34](#)
- [Displaying the NTP Configuration, page 5-35](#)

Default NTP Configuration

[Table 5-4](#) shows the default NTP configuration.

Table 5-4 **Default NTP Configuration**

Feature	Default Setting
NTP authentication	Disabled. No authentication key is specified.
NTP peer or server associations	None configured.
NTP broadcast service	Disabled; no interface sends or receives NTP broadcast packets.
NTP access restrictions	No access control is specified.
NTP packet source IP address	The source address is determined by the outgoing interface.

NTP is disabled by default.

Configuring NTP Authentication

This procedure must be coordinated with the administrator of the NTP server; the information you configure in this procedure must be matched by the servers used by the access point/bridge to synchronize its time to the NTP server.

Beginning in privileged EXEC mode, follow these steps to authenticate the associations (communications between devices running NTP that provide for accurate timekeeping) with other devices for security purposes:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	ntp authenticate	Enable the NTP authentication feature, which is disabled by default.

	Command	Purpose
Step 3	ntp authentication-key <i>number</i> md5 <i>value</i>	Define the authentication keys. By default, none are defined. - For <i>number</i>, specify a key number. The range is 1 to 4294967295. md5 specifies that message authentication support is provided by using the message digest algorithm 5 (MD5). - For <i>value</i>, enter an arbitrary string of up to eight characters for the key. The access point/bridge does not synchronize to a device unless both have one of these authentication keys, and the key number is specified by the ntp trusted-key <i>key-number</i> command.
Step 4	ntp trusted-key <i>key-number</i>	Specify one or more key numbers (defined in Step 3) that a peer NTP device must provide in its NTP packets for this access point/bridge to synchronize to it. By default, no trusted keys are defined. For <i>key-number</i>, specify the key defined in Step 3. This command provides protection against accidentally synchronizing the access point/bridge to a device that is not trusted.
Step 5	end	Return to privileged EXEC mode.
Step 6	show running-config	Verify your entries.
Step 7	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To disable NTP authentication, use the **no ntp authenticate** global configuration command. To remove an authentication key, use the **no ntp authentication-key** *number* global configuration command. To disable authentication of the identity of a device, use the **no ntp trusted-key** *key-number* global configuration command.

This example shows how to configure the access point/bridge to synchronize only to devices providing authentication key 42 in the device's NTP packets:

```
ap(config)# ntp authenticate
ap(config)# ntp authentication-key 42 md5 aNiceKey
ap(config)# ntp trusted-key 42
```

Configuring NTP Associations

An NTP association can be a peer association (this access point/bridge can either synchronize to the other device or allow the other device to synchronize to it), or it can be a server association (meaning that only this access point/bridge synchronizes to the other device, and not the other way around).

Beginning in privileged EXEC mode, follow these steps to form an NTP association with another device:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	ntp peer <i>ip-address</i> [version <i>number</i>] [key <i>keyid</i>] [source <i>interface</i>] [prefer]	Configure the access point/bridge system clock to synchronize a peer or to be synchronized by a peer (peer association).
	or ntp server <i>ip-address</i> [version <i>number</i>] [key <i>keyid</i>] [source <i>interface</i>] [prefer]	Configure the access point/bridge system clock to be synchronized by a time server (server association). No peer or server associations are defined by default. - For <i>ip-address</i> in a peer association, specify either the IP address of the peer providing, or being provided, the clock synchronization. For a server association, specify the IP address of the time server providing the clock synchronization. (Optional) For <i>number</i>, specify the NTP version number. The range is 1 to 3. By default, version 3 is selected. (Optional) For <i>keyid</i>, enter the authentication key defined with the ntp authentication-key global configuration command. (Optional) For <i>interface</i>, specify the interface from which to pick the IP source address. By default, the source IP address is taken from the outgoing interface. (Optional) Enter the prefer keyword to make this peer or server the preferred one that provides synchronization. This keyword reduces switching back and forth between peers and servers.
Step 3	end	Return to privileged EXEC mode.
Step 4	show running-config	Verify your entries.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

You need to configure only one end of an association; the other device can automatically establish the association. If you are using the default NTP version (version 3) and NTP synchronization does not occur, try using NTP version 2. Many NTP servers on the Internet run version 2.

To remove a peer or server association, use the **no ntp peer** *ip-address* or the **no ntp server** *ip-address* global configuration command.

This example shows how to configure the access point/bridge to synchronize its system clock with the clock of the peer at IP address 172.16.22.44 using NTP version 2:

```
ap(config)# ntp server 172.16.22.44 version 2
```

Configuring NTP Broadcast Service

The communications between devices running NTP (known as *associations*) are usually statically configured; each device is given the IP addresses of all devices with which it should form associations. Accurate timekeeping is possible by exchanging NTP messages between each pair of devices with an association. However, in a LAN environment, NTP can be configured to use IP broadcast messages instead. This alternative reduces configuration complexity because each device can simply be configured to send or receive broadcast messages. However, the information flow is one-way only.

The access point/bridge can send or receive NTP broadcast packets on an interface-by-interface basis if there is an NTP broadcast server, such as a router, broadcasting time information on the network. The access point/bridge can send NTP broadcast packets to a peer so that the peer can synchronize to it. The access point/bridge can also receive NTP broadcast packets to synchronize its own clock. This section provides procedures for both sending and receiving NTP broadcast packets.

Beginning in privileged EXEC mode, follow these steps to configure the access point/bridge to send NTP broadcast packets to peers so that they can synchronize their clock to the access point/bridge:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface <i>interface-id</i>	Enter interface configuration mode, and specify the interface to send NTP broadcast packets.
Step 3	ntp broadcast [<i>version number</i>] [<i>key keyid</i>] [<i>destination-address</i>]	Enable the interface to send NTP broadcast packets to a peer. By default, this feature is disabled on all interfaces. (Optional) For <i>number</i>, specify the NTP version number. The range is 1 to 3. If you do not specify a version, version 3 is used. (Optional) For <i>keyid</i>, specify the authentication key to use when sending packets to the peer. (Optional) For <i>destination-address</i>, specify the IP address of the peer that is synchronizing its clock to this access point/bridge.
Step 4	end	Return to privileged EXEC mode.
Step 5	show running-config	Verify your entries.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.
Step 7		Configure the connected peers to receive NTP broadcast packets as described in the next procedure.

To disable the interface from sending NTP broadcast packets, use the **no ntp broadcast** interface configuration command.

This example shows how to configure an interface to send NTP version 2 packets:

```
ap(config)# interface ethernet0/1
ap(config-if)# ntp broadcast version 2
```

Beginning in privileged EXEC mode, follow these steps to configure the access point/bridge to receive NTP broadcast packets from connected peers:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface <i>interface-id</i>	Enter interface configuration mode, and specify the interface to receive NTP broadcast packets.
Step 3	ntp broadcast client	Enable the interface to receive NTP broadcast packets. By default, no interfaces receive NTP broadcast packets.
Step 4	exit	Return to global configuration mode.
Step 5	ntp broadcastdelay <i>microseconds</i>	(Optional) Change the estimated round-trip delay between the access point/bridge and the NTP broadcast server. The default is 3000 microseconds; the range is 1 to 999999.
Step 6	end	Return to privileged EXEC mode.
Step 7	show running-config	Verify your entries.
Step 8	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To disable an interface from receiving NTP broadcast packets, use the **no ntp broadcast client** interface configuration command. To change the estimated round-trip delay to the default, use the **no ntp broadcastdelay** global configuration command.

This example shows how to configure an interface to receive NTP broadcast packets:

```
ap(config)# interface ethernet0/1
ap(config-if)# ntp broadcast client
```

Configuring NTP Access Restrictions

You can control NTP access on two levels as described in these sections:

- [Creating an Access Group and Assigning a Basic IP Access List, page 5-33](#)
- [Disabling NTP Services on a Specific Interface, page 5-34](#)

Creating an Access Group and Assigning a Basic IP Access List

Beginning in privileged EXEC mode, follow these steps to control access to NTP services by using access lists:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	ntp access-group {query-only serve-only serve peer} <i>access-list-number</i>	Create an access group, and apply a basic IP access list. The keywords have these meanings: • query-only—Allows only NTP control queries. • serve-only—Allows only time requests. • serve—Allows time requests and NTP control queries, but does not allow the access point/bridge to synchronize to the remote device. • peer—Allows time requests and NTP control queries and allows the access point/bridge to synchronize to the remote device. For <i>access-list-number</i>, enter a standard IP access list number from 1 to 99.
Step 3	access-list access-list-number permit <i>source [source-wildcard]</i>	Create the access list. • For <i>access-list-number</i>, enter the number specified in Step 2. • Enter the permit keyword to permit access if the conditions are matched. • For <i>source</i>, enter the IP address of the device that is permitted access to the access point/bridge. • (Optional) For <i>source-wildcard</i>, enter the wildcard bits to be applied to the source. Note When creating an access list, remember that, by default, the end of the access list contains an implicit deny statement for everything if it did not find a match before reaching the end.
Step 4	end	Return to privileged EXEC mode.
Step 5	show running-config	Verify your entries.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

The access group keywords are scanned in this order, from least restrictive to most restrictive:

1. **peer**—Allows time requests and NTP control queries and allows the access point/bridge to synchronize itself to a device whose address passes the access list criteria.
2. **serve**—Allows time requests and NTP control queries, but does not allow the access point/bridge to synchronize itself to a device whose address passes the access list criteria.
3. **serve-only**—Allows only time requests from a device whose address passes the access list criteria.
4. **query-only**—Allows only NTP control queries from a device whose address passes the access list criteria.

If the source IP address matches the access lists for more than one access type, the first type is granted. If no access groups are specified, all access types are granted to all devices. If any access groups are specified, only the specified access types are granted.

To remove access control to the access point/bridge NTP services, use the **no ntp access-group {query-only | serve-only | serve | peer}** global configuration command.

This example shows how to configure the access point/bridge to allow itself to synchronize to a peer from access list 99. However, the access point/bridge restricts access to allow only time requests from access list 42:

```
ap# configure terminal
ap(config)# ntp access-group peer 99
ap(config)# ntp access-group serve-only 42
ap(config)# access-list 99 permit 172.20.130.5
ap(config)# access list 42 permit 172.20.130.6
```

Disabling NTP Services on a Specific Interface

NTP services are enabled on all interfaces by default.

Beginning in privileged EXEC mode, follow these steps to disable NTP packets from being received on an interface:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface <i>interface-id</i>	Enter interface configuration mode, and specify the interface to disable.
Step 3	ntp disable	Disable NTP packets from being received on the interface. By default, all interfaces receive NTP packets.
Step 4	end	Return to privileged EXEC mode.
Step 5	show running-config	Verify your entries.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To re-enable receipt of NTP packets on an interface, use the **no ntp disable** interface configuration command.

Configuring the Source IP Address for NTP Packets

When the access point/bridge sends an NTP packet, the source IP address is normally set to the address of the interface through which the NTP packet is sent. Use the **ntp source** global configuration command when you want to use a particular source IP address for all NTP packets. The address is taken from the specified interface. This command is useful if the address on an interface cannot be used as the destination for reply packets.

Beginning in privileged EXEC mode, follow these steps to configure a specific interface from which the IP source address is to be taken:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	ntp source <i>type number</i>	Specify the interface type and number from which the IP source address is taken. By default, the source address is determined by the outgoing interface.
Step 3	end	Return to privileged EXEC mode.
Step 4	show running-config	Verify your entries.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

The specified interface is used for the source address for all packets sent to all destinations. If a source address is to be used for a specific association, use the **source** keyword in the **ntp peer** or **ntp server** global configuration command as described in the [“Configuring NTP Associations”](#) section on page 5-30.

Displaying the NTP Configuration

You can use two privileged EXEC commands to display NTP information:

- **show ntp associations [detail]**
- **show ntp status**

For detailed information about the fields in these displays, refer to the *Cisco IOS Configuration Fundamentals Command Reference for Release 12.3*.

Configuring Time and Date Manually

If no other source of time is available, you can manually configure the time and date after the system is restarted. The time remains accurate until the next system restart. We recommend that you use manual configuration only as a last resort. If you have an outside source to which the access point/bridge can synchronize, you do not need to manually set the system clock.

This section contains this configuration information:

- [Setting the System Clock, page 5-35](#)
- [Displaying the Time and Date Configuration, page 5-36](#)
- [Configuring the Time Zone, page 5-36](#)
- [Configuring Summer Time \(Daylight Saving Time\), page 5-37](#)

Setting the System Clock

If you have an outside source on the network that provides time services, such as an NTP server, you do not need to manually set the system clock.

Beginning in privileged EXEC mode, follow these steps to set the system clock:

	Command	Purpose
Step 1	clock set <i>hh:mm:ss day month year</i> or clock set <i>hh:mm:ss month day year</i>	Manually set the system clock using one of these formats. - For <i>hh:mm:ss</i>, specify the time in hours (24-hour format), minutes, and seconds. The time specified is relative to the configured time zone. - For <i>day</i>, specify the day by date in the month. - For <i>month</i>, specify the month by name. - For <i>year</i>, specify the year (no abbreviation).
Step 2	show running-config	Verify your entries.
Step 3	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to manually set the system clock to 1:32 p.m. on July 23, 2001:

```
ap# clock set 13:32:00 23 July 2001
```

Displaying the Time and Date Configuration

To display the time and date configuration, use the **show clock [detail]** privileged EXEC command.

The system clock keeps an *authoritative* flag that shows whether the time is authoritative (believed to be accurate). If the system clock has been set by a timing source such as NTP, the flag is set. If the time is not authoritative, it is used only for display purposes. Until the clock is authoritative and the *authoritative* flag is set, the flag prevents peers from synchronizing to the clock when the peers' time is invalid.

The symbol that precedes the **show clock** display has this meaning:

- *—Time is not authoritative.
- (blank)—Time is authoritative.
- .—Time is authoritative, but NTP is not synchronized.

Configuring the Time Zone

Beginning in privileged EXEC mode, follow these steps to manually configure the time zone:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	clock timezone <i>zone hours-offset</i> [<i>minutes-offset</i>]	Set the time zone. The access point/bridge keeps internal time in universal time coordinated (UTC), so this command is used only for display purposes and when the time is manually set. - For <i>zone</i>, enter the name of the time zone to be displayed when standard time is in effect. The default is UTC. - For <i>hours-offset</i>, enter the hours offset from UTC. (Optional) For <i>minutes-offset</i>, enter the minutes offset from UTC.

	Command	Purpose
Step 3	end	Return to privileged EXEC mode.
Step 4	show running-config	Verify your entries.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

The *minutes-offset* variable in the **clock timezone** global configuration command is available for those cases where a local time zone is a percentage of an hour different from UTC. For example, the time zone for some sections of Atlantic Canada (AST) is UTC-3.5, where the 3 means 3 hours and .5 means 50 percent. In this case, the necessary command is **clock timezone AST -3 30**.

To set the time to UTC, use the **no clock timezone** global configuration command.

Configuring Summer Time (Daylight Saving Time)

Beginning in privileged EXEC mode, follow these steps to configure summer time (daylight saving time) in areas where it starts and ends on a particular day of the week each year:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	clock summer-time zone recurring [<i>week day month hh:mm week day month hh:mm [offset]</i>]	Configure summer time to start and end on the specified days every year. Summer time is disabled by default. If you specify clock summer-time zone recurring without parameters, the summer time rules default to the United States rules. - For <i>zone</i>, specify the name of the time zone (for example, PDT) to be displayed when summer time is in effect. (Optional) For <i>week</i>, specify the week of the month (1 to 5 or last). (Optional) For <i>day</i>, specify the day of the week (Sunday, Monday...). (Optional) For <i>month</i>, specify the month (January, February...). (Optional) For <i>hh:mm</i>, specify the time (24-hour format) in hours and minutes. (Optional) For <i>offset</i>, specify the number of minutes to add during summer time. The default is 60.
Step 3	end	Return to privileged EXEC mode.
Step 4	show running-config	Verify your entries.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

The first part of the **clock summer-time** global configuration command specifies when summer time begins, and the second part specifies when it ends. All times are relative to the local time zone. The start time is relative to standard time. The end time is relative to summer time. If the starting month is after the ending month, the system assumes that you are in the southern hemisphere.

This example shows how to specify that summer time starts on the first Sunday in April at 02:00 and ends on the last Sunday in October at 02:00:

```
ap(config)# clock summer-time PDT recurring 1 Sunday April 2:00 last Sunday October 2:00
```

Beginning in privileged EXEC mode, follow these steps if summer time in your area does not follow a recurring pattern (configure the exact date and time of the next summer time events):

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	clock summer-time zone date [month date year hh:mm month date year hh:mm [offset]] or clock summer-time zone date [date month year hh:mm date month year hh:mm [offset]]	Configure summer time to start on the first date and end on the second date. Summer time is disabled by default. - For <i>zone</i>, specify the name of the time zone (for example, PDT) to be displayed when summer time is in effect. (Optional) For <i>week</i>, specify the week of the month (1 to 5 or last). (Optional) For <i>day</i>, specify the day of the week (Sunday, Monday...). (Optional) For <i>month</i>, specify the month (January, February...). (Optional) For <i>hh:mm</i>, specify the time (24-hour format) in hours and minutes. (Optional) For <i>offset</i>, specify the number of minutes to add during summer time. The default is 60.
Step 3	end	Return to privileged EXEC mode.
Step 4	show running-config	Verify your entries.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

The first part of the **clock summer-time** global configuration command specifies when summer time begins, and the second part specifies when it ends. All times are relative to the local time zone. The start time is relative to standard time. The end time is relative to summer time. If the starting month is after the ending month, the system assumes that you are in the southern hemisphere.

To disable summer time, use the **no clock summer-time** global configuration command.

This example shows how to set summer time to start on October 12, 2000, at 02:00, and end on April 26, 2001, at 02:00:

```
bridge(config)# clock summer-time pdt date 12 October 2000 2:00 26 April 2001 2:00
```

Configuring a System Name and Prompt

You configure the system name on the access point/bridge to identify it. By default, the system name and prompt are *bridge*.

If you have not configured a system prompt, the first 20 characters of the system name are used as the system prompt. A greater-than symbol (>) is appended. The prompt is updated whenever the system name changes, unless you manually configure the prompt by using the **prompt** global configuration command.



Note

For complete syntax and usage information for the commands used in this section, refer to the *Cisco IOS Configuration Fundamentals Command Reference* and the *Cisco IOS IP and IP Routing Command Reference for Release 12.3*.

This section contains this configuration information:

- [Default System Name and Prompt Configuration, page 5-39](#)
- [Configuring a System Name, page 5-39](#)
- [Understanding DNS, page 5-39](#)

Default System Name and Prompt Configuration

The default access point/bridge system name and prompt is *bridge*.

Configuring a System Name

Beginning in privileged EXEC mode, follow these steps to manually configure a system name:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	hostname <i>name</i>	Manually configure a system name. The default setting is <i>bridge</i> . The name must follow the rules for ARPANET host names. They must start with a letter, end with a letter or digit, and have as interior characters only letters, digits, and hyphens. Names can be up to 63 characters.
Step 3	end	Return to privileged EXEC mode.
Step 4	show running-config	Verify your entries.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

When you set the system name, it is also used as the system prompt.

To return to the default host name, use the **no hostname** global configuration command.

Understanding DNS

The DNS protocol controls the Domain Name System (DNS), a distributed database with which you can map host names to IP addresses. When you configure DNS on your access point/bridge, you can substitute the host name for the IP address with all IP commands, such as **ping**, **telnet**, **connect**, and related Telnet support operations.

IP defines a hierarchical naming scheme that allows a device to be identified by its location or domain. Domain names are pieced together with periods (.) as the delimiting characters. For example, Cisco Systems is a commercial organization that IP identifies by a *com* domain name, so its domain name is *cisco.com*. A specific device in this domain, such as the File Transfer Protocol (FTP) system, is identified as *ftp.cisco.com*.

To keep track of domain names, IP has defined the concept of a domain name server, which holds a cache (or database) of names mapped to IP addresses. To map domain names to IP addresses, you must first identify the host names, specify the name server that is present on your network, and enable the DNS.

This section contains this configuration information:

- [Default DNS Configuration, page 5-40](#)
- [Setting Up DNS, page 5-40](#)
- [Displaying the DNS Configuration, page 5-41](#)

Default DNS Configuration

[Table 5-5](#) shows the default DNS configuration.

Table 5-5 **Default DNS Configuration**

Feature	Default Setting
DNS enable state	Disabled.
DNS default domain name	None configured.
DNS servers	No name server addresses are configured.

Setting Up DNS

Beginning in privileged EXEC mode, follow these steps to set up your access point/bridge to use the DNS:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	ip domain-name <i>name</i>	Define a default domain name that the software uses to complete unqualified host names (names without a dotted-decimal domain name). Do not include the initial period that separates an unqualified name from the domain name. At boot time, no domain name is configured; however, if the access point/bridge configuration comes from a BOOTP or Dynamic Host Configuration Protocol (DHCP) server, then the default domain name might be set by the BOOTP or DHCP server (if the servers were configured with this information).
Step 3	ip name-server <i>server-address1</i> [<i>server-address2</i> ... <i>server-address6</i>]	Specify the address of one or more name servers to use for name and address resolution. You can specify up to six name servers. Separate each server address with a space. The first server specified is the primary server. The access point/bridge sends DNS queries to the primary server first. If that query fails, the backup servers are queried.
Step 4	ip domain-lookup	(Optional) Enable DNS-based host name-to-address translation on your access point/bridge. This feature is enabled by default. If your network devices require connectivity with devices in networks for which you do not control name assignment, you can dynamically assign device names that uniquely identify your devices by using the global Internet naming scheme (DNS).
Step 5	end	Return to privileged EXEC mode.

	Command	Purpose
Step 6	show running-config	Verify your entries.
Step 7	copy running-config startup-config	(Optional) Save your entries in the configuration file.

If you use the access point/bridge IP address as its host name, the IP address is used and no DNS query occurs. If you configure a host name that contains no periods (.), a period followed by the default domain name is appended to the host name before the DNS query is made to map the name to an IP address. The default domain name is the value set by the **ip domain-name** global configuration command. If there is a period (.) in the host name, the IOS software looks up the IP address without appending any default domain name to the host name.

To remove a domain name, use the **no ip domain-name** *name* global configuration command. To remove a name server address, use the **no ip name-server** *server-address* global configuration command. To disable DNS on the access point/bridge, use the **no ip domain-lookup** global configuration command.

Displaying the DNS Configuration

To display the DNS configuration information, use the **show running-config** privileged EXEC command.

Creating a Banner

You can configure a message-of-the-day (MOTD) and a login banner. The MOTD banner appears on all connected terminals at login and is useful for sending messages that affect all network users (such as impending system shutdowns).

The login banner also appears on all connected terminals. It appears after the MOTD banner and before the login prompts.



Note

For complete syntax and usage information for the commands used in this section, refer to the *Cisco IOS Configuration Fundamentals Command Reference for Release 12.2*.

This section contains this configuration information:

- [Default Banner Configuration, page 5-41](#)
- [Configuring a Message-of-the-Day Login Banner, page 5-41](#)
- [Configuring a Login Banner, page 5-42](#)

Default Banner Configuration

The MOTD and login banners are not configured.

Configuring a Message-of-the-Day Login Banner

You can create a single or multiline message banner that appears on the screen when someone logs into the access point/bridge.

Beginning in privileged EXEC mode, follow these steps to configure a MOTD login banner:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	banner motd <i>c message c</i>	Specify the message of the day. For <i>c</i> , enter the delimiting character of your choice, such as a pound sign (#), and press the Return key. The delimiting character signifies the beginning and end of the banner text. Characters after the ending delimiter are discarded. For <i>message</i> , enter a banner message up to 255 characters. You cannot use the delimiting character in the message.
Step 3	end	Return to privileged EXEC mode.
Step 4	show running-config	Verify your entries.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To delete the MOTD banner, use the **no banner motd** global configuration command.

This example shows how to configure a MOTD banner for the access point/bridge using the pound sign (#) symbol as the beginning and ending delimiter:

```
ap(config)# banner motd #
This is a secure site. Only authorized users are allowed.
For access, contact technical support.
#
ap(config)#
```

This example shows the banner displayed from the previous configuration:

```
Unix> telnet 172.2.5.4
Trying 172.2.5.4...
Connected to 172.2.5.4.
Escape character is '^]'.
```

```
This is a secure site. Only authorized users are allowed.
For access, contact technical support.
```

```
User Access Verification
```

```
Password:
```

Configuring a Login Banner

You can configure a login banner to appear on all connected terminals. This banner appears after the MOTD banner and before the login prompt.

Beginning in privileged EXEC mode, follow these steps to configure a login banner:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	banner login <i>c message c</i>	Specify the login message. For <i>c</i> , enter the delimiting character of your choice, such as a pound sign (#), and press the Return key. The delimiting character signifies the beginning and end of the banner text. Characters after the ending delimiter are discarded. For <i>message</i> , enter a login message up to 255 characters. You cannot use the delimiting character in the message.
Step 3	end	Return to privileged EXEC mode.
Step 4	show running-config	Verify your entries.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To delete the login banner, use the **no banner login** global configuration command.

This example shows how to configure a login banner for the access point/bridge using the dollar sign (\$) symbol as the beginning and ending delimiter:

```
ap(config)# banner login $
Access for authorized users only. Please enter your username and password.
$
ap(config)#
```




Configuring Radio Settings

This chapter describes how to configure radio settings for your access point/bridge. This chapter includes these sections:

- [Enabling the Radio Interface, page 6-2](#)
- [Configuring the Role in Radio Network, page 6-2](#)
- [Configuring Radio Data Rates, page 6-5](#)
- [Configuring Radio Transmit Power, page 6-7](#)
- [Configuring Radio Channel Settings, page 6-9](#)
- [Enabling and Disabling World Mode, page 6-11](#)
- [Disabling and Enabling Short Radio Preambles, page 6-12](#)
- [Configuring Transmit and Receive Antennas, page 6-13](#)
- [Aironet Extensions, page 6-14](#)
- [Configuring the Ethernet Encapsulation Transformation Method, page 6-15](#)
- [Enabling and Disabling Concatenation, page 6-15](#)
- [Configuring the Radio Distance Setting, page 6-16](#)
- [Enabling and Disabling Reliable Multicast to Workgroup Bridges, page 6-16](#)
- [Enabling and Disabling Public Secure Packet Forwarding, page 6-17](#)
- [Enabling Short Slot Time, page 6-19](#)
- [Configuring the Beacon Period and the DTIM, page 6-19](#)
- [Configure RTS Threshold and Retries, page 6-19](#)
- [Configuring the Maximum Data Retries, page 6-20](#)
- [Configuring the Fragmentation Threshold, page 6-21](#)
- [Setting the Root Parent Timeout Value, page 6-21](#)
- [Configuring the Root Parent MAC, page 6-22](#)
- [Performing a Carrier Busy Test, page 6-22](#)

Enabling the Radio Interface

The radio interface is disabled by default.

**Note**

In Cisco IOS Release 12.3(7)JA there is no default SSID. You must create an SSID before you can enable the radio interface.

Beginning in privileged EXEC mode, follow these steps to enable the access point/bridge radio:

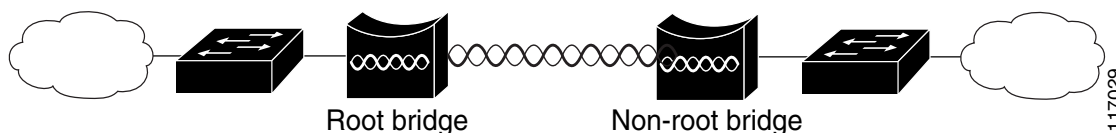
	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.
Step 3	ssid <i>string</i>	Enter the Radio Service Set Identifier. The SSID can consist of up to 32 alphanumeric characters. SSIDs are case sensitive.
Step 4	end	Return to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

The radio is enabled when you set the SSID.

Configuring the Role in Radio Network

You can configure your access point/bridge as a root bridge, non-root bridge, access point, or workgroup bridge. [Figure 6-1](#) shows a root bridge communicating with a non-root bridge in a point-to-point configuration.

Figure 6-1 Point-to-Point Bridge Configuration



[Figure 6-2](#) shows a typical configuration where the bridge functions as an access point.

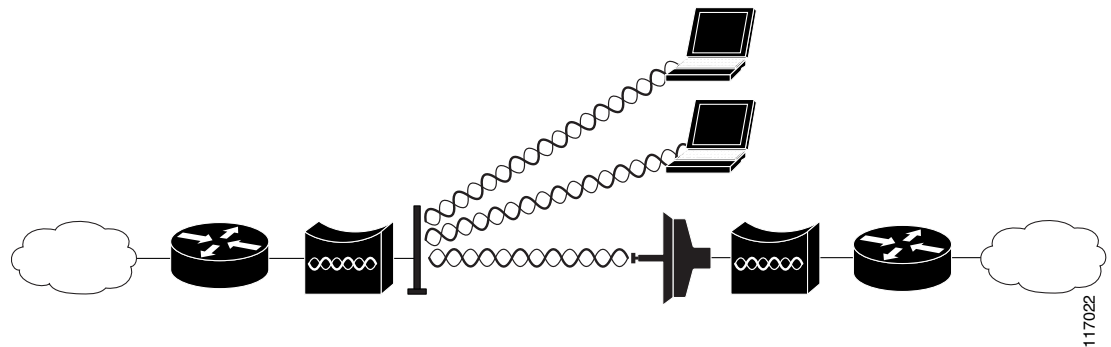
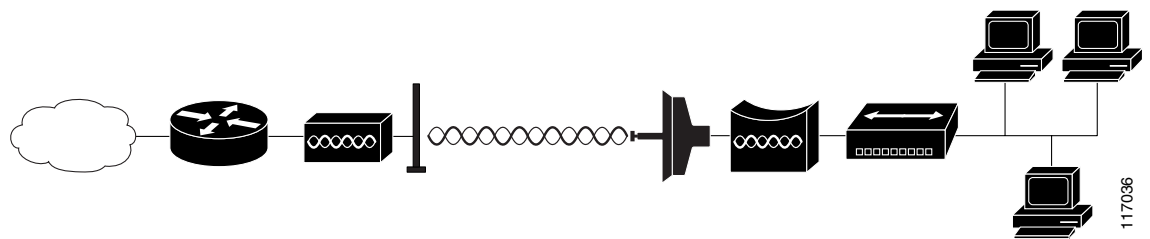
Figure 6-2 Access Point Configuration

Figure 6-3 shows how the bridge performs when configured as a workgroup bridge.

Figure 6-3 Workgroup Bridge Configuration

Beginning in privileged EXEC mode, follow these steps to set the access point/bridge's radio network role:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.

	Command	Purpose
Step 3	station role install {automatic non-root root} non-root {bridge wireless clients} repeater root {access-point ap-only [bridge wireless-clients] [fallback repeater shutdown]} scanner workgroup-bridge	Set the access point/bridge role. • install—Places the access point/bridge in a bridge link setup mode for antenna alignment purposes. The automatic option configures the access point/bridge to automatically search for a link to another access point/bridge or an access point in bridge mode. The root and non-root options allow you to manually configure the access point/bridge. • non-root—Places the access point/bridge in non-root bridge mode. The wireless clients option allows clients to associate to the non-root access point/bridge while it is in the non-root bridge mode. • root—Places the access point/bridge in root bridge mode. The ap-only option makes the access point act as a root access point (the default station role). • scanner—Causes the access point/bridge to operate as a scanner only and does not accept associations from client devices. As a scanner, the access point/bridge collects radio data and sends it to the WDS server on your network. Note The scanner mode is supported only when used with a WLSE device on your network. • workgroup-bridge—Places the access point/bridge in the workgroup bridge mode. As a workgroup bridge, the access point/bridge associates to an access point or bridge as a client and provides a wireless LAN connection for devices connected to its Ethernet port.
Step 4	mobile station	(Optional) Use this command to configure a non-root bridge as a mobile station. When this feature is enabled the non-root bridge scans for a new parent association when it encounters a poor Received Signal Strength Indicator (RSSI), excessive radio interference, or a high frame-loss percentage. Using these criteria, the access point/bridge searches for a new root association and roams to a new root bridge before it loses its current association. When the mobile station setting is disabled (the default setting) the bridge does not search for a new association until it loses its current association.
Step 5	end	Return to privileged EXEC mode.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

**Note**

See [Chapter 20, “Configuring Repeater and Standby Access Points and Workgroup Bridge Mode,”](#) for more information about configuring the access point/bridge as an access point or workgroup bridge.

Configuring Radio Data Rates

You use the data rate settings to choose the data rates the access point/bridge uses for data transmission. The rates are expressed in megabits per second. The access point/bridge always attempts to transmit at the highest data rate set to **Basic**, also called **Require** on the browser-based interface. If there are obstacles or interference, the access point/bridge steps down to the highest rate that allows data transmission. You can set each data rate to one of three states:

- **Basic** (this is the default state for all data rates)—Allows transmission at this rate for all packets, both unicast and multicast. At least one of the access point/bridge's data rates must be set to Basic.
- **Enabled**—The access point/bridge transmits only unicast packets at this rate; multicast packets are sent at one of the data rates set to Basic.
- **Disabled**—The access point/bridge does not transmit data at this rate.

**Note**

At least one data rate must be set to **basic**.

You can use the Data Rate settings to set the access point/bridge to serve client devices operating at specific data rates. For example, to set the 2.4-GHz radio for 11 megabits per second (Mbps) service only, set the 11-Mbps rate to **Basic** and set the other data rates to **Disabled**. To set the wireless device to serve only client devices operating at 1 and 2 Mbps, set 1 and 2 to **Basic** and set the rest of the data rates to **Disabled**. To set the 2.4-GHz, 802.11g radio to serve only 802.11g client devices, set any Orthogonal Frequency Division Multiplexing (OFDM) data rate (6, 9, 12, 18, 24, 36, 48, 54) to **Basic**.

You can also configure the access point/bridge to set the data rates automatically to optimize either range or throughput. When you enter **range** for the data rate setting, the access point/bridge sets the 6-Mbps rate to **basic** and the other rates to **enabled**. When you enter **throughput** for the data rate setting, the access point/bridge sets all data rates to **basic**. Enter **default** to set the data rates to factory defaults.

Beginning in privileged EXEC mode, follow these steps to configure the radio data rates:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.

	Command	Purpose
Step 3	speed { [1.0] [2.0] [5.5] [6.0] [9.0] [11.0] [12.0] [18.0] [24.0] [36.0] [48.0] [54.0] [basic-1.0] [basic-2.0] [basic-5.5] [basic-6.0] [basic-9.0] [basic-11.0] [basic-12.0] [basic-18.0] [basic-24.0] [basic-36.0] [basic-48.0] [basic-54.0] range throughput [ofdm] default }	Set each data rate to basic or enabled, or enter range to optimize range or throughput to optimize throughput. - Enter 1.0, 2.0, 5.5, 6.0, 9.0, 11.0, 12.0, 18.0, 24.0, 36.0, 48.0, and 54.0 to set these data rates to enabled on the 802.11g, 2.4-GHz radio. Enter basic-1.0, basic-2.0, basic-5.5, basic-6.0, basic-9.0, basic-11.0, basic-12.0, basic-18.0, basic-24.0, basic-36.0, basic-48.0, and basic-54.0 to set these data rates to basic on the 802.11g, 2.4-GHz radio. Note The client must support the basic rate that you select or it cannot associate to the wireless device. If you select 12 Mbps or higher for the basic data rate on the 802.11g radio, 802.11b client devices cannot associate to the wireless device 802.11g radio. (Optional) Enter range or throughput or ofdm-throughput (no ERP protection) to automatically optimize radio range or throughput. When you enter range, the wireless device sets the lowest data rate to basic and the other rates to enabled. When you enter throughput, the wireless device sets all data rates to basic. (Optional) Enter speed throughput ofdm to set all OFDM rates (6, 9, 12, 18, 24, 36, and 48) to basic (required) and set all the CCK rates (1, 2, 5.5, and 11) to disabled. This setting disables 802.11b protection mechanisms and provides maximum throughput for 802.11g clients. However, it prevents 802.11b clients from associating to the access point. (Optional) Enter default to set the data rates to factory default settings (not supported on 802.11b radios). On the 802.11g radio, the default option sets rates 1, 2, 5.5, and 11 to basic, and rates 6, 9, 12, 18, 24, 36, 48, and 54 to enabled. These rate settings allow both 802.11b and 802.11g client devices to associate to the wireless device 802.11g radio.
Step 4	end	Return to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Use the **no** form of the **speed** command to disable data rates. When you use the **no** form of the command, all data rates are disabled except the rates you name in the command. This example shows how to disable data rate 6.0:

```
ap# configure terminal
ap(config)# interface dot11radio 0
ap(config-if)# no speed basic-9.0 basic-12.0 basic-18.0 basic-24.0 basic-36.0 basic-48.0
basic-54.0
ap(config-if)# end
```

Data rate 6 is disabled, and the rest of the rates are set to basic.

This example shows how to set up the access point/bridge for 54-Mbps service only:

```

ap# configure terminal
ap(config)# interface dot11radio 0
ap(config-if)# speed basic-54.0
ap(config-if)# end

```

Data rate 54 is set to basic, and the rest of the data rates are set to enabled.

Configuring Radio Transmit Power

Radio transmit power is based on the radio installed in your access point/ and the regulatory domain in which it operates. Rather than listing all transmit power variations for every regulatory domain, an example that shows how to configure radio transmit power is provided.

To determine what transmit power is available for a your access point and regulatory domain operate it in, refer to the hardware installation guide for that device. Hardware installation guides are available at cisco.com. Follow these steps to view and download them:

-
- Step 1** Browse to <http://www.cisco.com>.
 - Step 2** Click **Technical Support & Documentation**. A small window appears containing a list of technical support links.
 - Step 3** Click **Technical Support & Documentation**. The Technical Support and Documentation page appears.
 - Step 4** In the Documentation & Tools section, choose **Wireless**. The Wireless Support Resources page appears.
 - Step 5** In the Wireless LAN Access section, choose the device you are working with. An introduction page for the device appears.
 - Step 6** In the Install and Upgrade section, choose **Install and Upgrade Guides**. The Install and Upgrade Guides page for the device appears.
 - Step 7** Choose the Hardware Installation Guide for the device. The home page for the guide appears.
 - Step 8** In the left frame, click **Channels and Antenna Settings**.
-

Table 6-1 shows the relationship between mW and dBm.

Table 6-1 Translation between mW and dBm

dBm	-1	2	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
mW	1	2	3	4	5	6	8	10	12	15	20	25	30	40	50	60	80	100	125	150	200	250

Beginning in privileged EXEC mode, follow these steps to set the transmit power on your access point/bridge radio:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.

	Command	Purpose
Step 3	power local cck { 1 5 10 20 30 50 100 maximum }	Set the transmit power for the 802.11g radio to one of the power levels allowed in your regulatory domain. All settings are in mW.
Step 4	power local ofdm { 1 5 10 20 30 maximum }	You can set Orthogonal Frequency Division Multiplexing (OFDM) power levels and Complementary Code Keying (CCK) power levels. CCK modulation is supported by 802.11b and 802.11g devices. OFDM modulation is supported by 802.11g devices. Note The settings allowed in your regulatory domain might differ from the settings listed here. Note The 802.11g radio transmits at up to 100 mW for the 1, 2, 5.5, and 11Mbps data rates. However, for the 6, 9, 12, 18, 24, 36, 48, and 54Mbps data rates, the maximum transmit power for the 802.11g radio is 30 mW.
Step 5	power client { 1 5 10 20 30 50 100 maximum }	Set the maximum power level allowed on client devices that associate to the access point/bridge in access point mode. All settings are in mW. Note The settings allowed in your regulatory domain might differ from the settings listed here.
Step 6	end	Return to privileged EXEC mode.
Step 7	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Use the **no** form of the power command to return the power setting to **maximum**, the default setting.

Limiting the Power Level for Associated Client Devices

You can also limit the power level on client devices that associate to the access point/bridge. When a client device associates to the access point/bridge, the access point/bridge sends the maximum power level setting to the client.

Beginning in privileged EXEC mode, follow these steps to specify a maximum allowed power setting on all client devices that associate to the access point/bridge:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio { <i>slot/port</i> }	Enter interface configuration mode for the radio interface.

	Command	Purpose
Step 3	power client These options are available for 802.11g, 2.4-GHz clients (in mW): [1 5 10 20 30 50 100 maximum] local [cck ofdm These cck power level options are available (in mW): [1 5 10 20 30 50 100 maximum] These ofdm power level options are available (in mW): [1 5 10 20 30 maximum]	Set the maximum power level allowed on client devices that associate to the wireless device. Note The settings allowed in your regulatory domain might differ from the settings listed here. Use the power local command to configure the access point/bridge radio power level. You can set Complementary Code Keying (CCK) or Orthogonal Frequency Division Multiplexing power levels.
Step 4	end	Return to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

**Note**

Aironet extensions must be enabled to limit the power level on associated client devices. Aironet extensions are enabled by default.

Configuring Radio Channel Settings

The default channel setting for the wireless device radios is least congested; at startup, the wireless device scans for and selects the least-congested channel. For most consistent performance after a site survey, however, we recommend that you assign a static channel setting for each access point. The channel settings on the wireless device correspond to the frequencies available in your regulatory domain. See the *Cisco Aironet 1300 Series Outdoor Access Point/Bridge Hardware Installation Guide* for the frequencies allowed in your domain.

Each 2.4-GHz 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. Both 802.11b and 802.11g 2.4-GHz radios use the same channels and frequencies.

**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.

Beginning in privileged EXEC mode, follow these steps to set the wireless device radio channel:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio { slot/port }	Enter interface configuration mode for the radio interface.

	Command	Purpose
Step 3	channel <i>frequency</i> least-congested	Set the default channel for the wireless device radio. Table 6-2 show the channels and frequencies. To search for the least-congested channel on startup, enter least-congested .
Step 4	end	Return to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

[Table 6-2](#) shows the available frequencies for the IEEE 802.11g 2.4-GHz radio.

Table 6-2 Channels and Available Frequencies for IEEE 802.11g 2.4 GHz Radio

Channel Identifier	Center Frequency (MHz)	Regulatory Domains							
		Americas (–A)		EMEA (–E)		Israel (–I)		Japan (–J)	
		CCK	OFDM	CCK	OFDM	CCK	OFDM	CCK	OFDM
1	2412	X	X	X	X	–	–	X	X
2	2417	X	X	X	X	–	–	X	X
3	2422	X	X	X	X	–	–	X	X
4	2427	X	X	X	X	–	–	X	X
5	2432	X	X	X	X	X	X	X	X
6	2437	X	X	X	X	X	X	X	X
7	2442	X	X	X	X	X	X	X	X
8	2447	X	X	X	X	X	X	X	X
9	2452	X	X	X	X	X	–	X	X
10	2457	X	X	X	X	X	–	X	X
11	2462	X	X	X	X	X	–	X	X
12	2467	–	–	X	X	X	–	X	X
13	2472	–	–	X	X	X	–	X	X
14	2484	–	–	–	–	–	–	–	–

Configuring LBS on Access Points

Use the CLI to configure LBS on your access point/bridge. Beginning in privileged EXEC mode, follow these steps to configure LBS:

Command	Purpose
configure terminal	Enter global configuration mode.
dot11 lbs <i>profile-name</i>	Create an LBS profile for the access point and enter LBS configuration mode.
server-address <i>ip-address</i> port <i>port</i>	Enter the IP address of the location server and the port on the server to which the access point sends UDP packets that contain location information.

Command	Purpose
<code>method { rssi }</code>	(Optional) Select the location method that the access point uses when reporting location information to the location server. In this release, <code>rssi</code> (in which the access point measures the location packet's RSSI) is the only option and is also the default.
<code>packet-type { short extended }</code>	(Optional) Select the packet type that the access point accepts from the LBS tag. short —The access point accepts short location packets from the tag. In short packets, the LBS information is missing from the tag packet's frame body and the packet indicates the tag's transmit channel. extended —This is the default setting. The access point accepts extended packets from the tag. An extended packet contains two bytes of LBS information in the frame body. If the packet does not contain those two bytes in the frame body, the access point drops the packet.
<code>channel-match</code>	(Optional) Specifies that the LBS packet sent by the tag must match the radio channel on which the access point receives the packet. If the channel used by the tag and the channel used by the access point do not match, the access point drops the packet. Channel match is enabled by default.
<code>multicast-address mac-address</code>	(Optional) Specifies the multicast address that the tag uses when it sends LBS packets. The default multicast address is <code>01:40:96:00:00:10</code> .
<code>interface dot11 { 0 1 }</code>	Specify the radio interface on which this LBS profile is enabled. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1. The profile remains inactive until you enter this command.
<code>exit</code>	Return to global configuration mode.

In this example, the profile *southside* is enabled on the access point's 802.11g radio:

```
ap# configure terminal
ap(config)# dot11 lbs southside
ap(dot11-lbs)# server-address 10.91.105.90 port 1066
ap(dot11-lbs)# interface dot11 0
ap(dot11-lbs)# exit
```

Enabling and Disabling World Mode

You can configure the access point/bridge to support 802.11d world mode or Cisco legacy world mode. When you enable world mode, the access point/bridge adds channel carrier set information to its beacon. Client devices with world mode enabled receive the carrier set information and adjust their settings automatically. For example, a client device used primarily in Japan could rely on world mode to adjust its channel and power settings automatically when it travels to Italy and joins a network there. Cisco

client devices running firmware version 5.30.17 or later detect whether the access point/bridge is using 802.11d or Cisco legacy world mode and automatically use world mode that matches the mode used by the access point/bridge. World mode is disabled by default.

Beginning in privileged EXEC mode, follow these steps to specify a maximum allowed power setting on all client devices that associate to the access point/bridge:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.
Step 3	power client These options are available for 802.11b, 2.4-GHz clients (in mW): { 1 5 20 30 50 100 maximum } These options are available for 802.11g, 2.4-GHz clients (in mW): { 1 5 10 20 30 50 100 maximum } world-mode dot11d country_code code { both indoor outdoor } legacy	Set the maximum power level allowed on client devices that associate to the access point/bridge. Note The settings allowed in your regulatory domain might differ from the settings listed here. Enable world mode. - Enter the dot11d option to enable 802.11d world mode. - When you enter the dot11d option, you must enter a two-character ISO country code (for example, the ISO country code for the United States is US). You can find a list of ISO country codes at the ISO website. - After the country code, you must enter indoor, outdoor, or both to indicate the placement of the access point/bridge. - Enter the legacy option to enable Cisco legacy world mode.
Step 4	end	Return to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Use the **no** form of the command to disable world mode.

Aironet extensions must be enabled for world mode operation. Aironet extensions are enabled by default.

Disabling and Enabling Short Radio Preambles

The radio preamble (sometimes called a *header*) is a section of data at the head of a packet that contains information that the access point and client devices need when sending and receiving packets. You can set the radio preamble to long or short:

- Short—A short preamble improves throughput performance. Cisco Aironet Wireless LAN Client Adapters support short preambles. Early models of Cisco Aironet's Wireless LAN Adapter (PC4800 and PC4800A) require long preambles.
- Long—A long preamble ensures compatibility between the access point/bridge and all early models of Cisco Aironet Wireless LAN Adapters (PC4800 and PC4800A). If these client devices do not associate to your access point/bridge, you should use short preambles.

You cannot configure short or long radio preambles on the 5-GHz radio.

Beginning in privileged EXEC mode, follow these steps to disable short radio preambles:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.
Step 3	no preamble-short	Disable short preambles and enable long preambles.
Step 4	end	Return to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Short preambles are enabled by default. Use the **preamble-short** command to enable short preambles if they are disabled.

Configuring Transmit and Receive Antennas

You can select the antenna the access point/bridge uses to receive and transmit data. There are three options for both the receive and the transmit antenna:

- **Diversity**—This default setting tells the access point/bridge to use the antenna that receives the best signal. If your access point/bridge has two fixed (non-removable) antennas, you should use this setting for both receive and transmit.
- **Right**—If your access point/bridge has removable antennas and you install a high-gain antenna on the access point/bridge's right connector, you should use this setting for both receive and transmit. When you look at the access point/bridge's back panel, the right antenna is on the right.
- **Left**—If your access point/bridge has removable antennas and you install a high-gain antenna on the access point/bridge's left connector, you should use this setting for both receive and transmit. When you look at the access point/bridge's back panel, the left antenna is on the left.



Note

The **antenna** commands are not available for access point/bridges equipped with a captive (internal) antenna.

Beginning in privileged EXEC mode, follow these steps to select the antennas the access point uses to receive and transmit data:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.

	Command	Purpose
Step 3	antenna gain {<-128 - 128>}	Specifies the antenna gain in dB of the connected antennas. Enter the gain in whole numbers (-128 –128 dBi) of the antenna(s) connected to your access point/bridge. Note This setting does not change the antenna gain, it is used to identify the gain of the installed antenna(s). Note The antenna gain value is listed on the user document that shipped with your antenna.
Step 4	antenna receive {diversity left right}	Set the receive antenna to diversity, left, or right. Note For best performance with two antennas, leave the receive antenna setting at the default setting, diversity . With one antenna, connect the antenna to the right connector and set the diversity to right .
Step 5	antenna transmit {diversity left right}	Set the transmit antenna to diversity, left, or right. Note For best performance with two antennas, leave the transmit antenna setting at the default setting, diversity . With one antenna, connect the antenna to the right connector and set the diversity to right .
Step 6	end	Return to privileged EXEC mode.
Step 7	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Aironet Extensions



Note

Aironet extensions are required by the access point/bridge. They cannot be disabled.

By default, the access point/bridge uses Cisco Aironet 802.11 extensions to detect the capabilities of Cisco Aironet client devices and to support features that require specific interaction between the access point/bridge and associated client devices. Aironet extensions must be enabled to support these features:

- Load balancing—The access point/bridge 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/bridge and all associated client devices, adds a few bytes to each packet to make the packets tamper-proof.
- Temporal Key Integrity Protocol (TKIP)—TKIP, also known as WEP key hashing, is an additional WEP security feature that defends against an attack on WEP in which the intruder uses an unencrypted segment called the initialization vector (IV) in encrypted packets to calculate the WEP key.
- Repeater mode—Aironet extensions must be enabled on repeater access points and on the root access points to which they associate.
- World mode—Client devices with world mode enabled receive carrier set information from the access point and adjust their settings automatically.

- Limiting the power level on associated client devices—When a client device associates to the access point/bridge, the access point/bridge sends the maximum allowed power level setting to the client.

Configuring the Ethernet Encapsulation Transformation Method

When the access point/bridge receives data packets that are not 802.3 packets, the access point/bridge must format the packets to 802.3 using an encapsulation transformation method. These are the two transformation methods:

- 802.1H—This method provides optimum performance for Cisco Aironet wireless products. This is the default setting.
- 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.

Beginning in privileged EXEC mode, follow these steps to configure the encapsulation transformation method:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.
Step 3	payload-encapsulation dot1h rfc1042	Set the encapsulation transformation method to RFC1042 (rfc1042) or 802.1h (dot1h , the default setting).
Step 4	end	Return to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.



Note

For best performance over your access point/bridge links, adjust the CW-min and CW-max contention window settings to depending on the number of non-root access point/bridges associated to each root access point/bridge. Refer to the [“CW-min and CW-max Settings for Point-to-Point and Point-to-Multipoint Bridge Links”](#) section on page 14-11 for instructions on adjusting these settings.

Enabling and Disabling Concatenation

Use the **concatenation** command to enable packet concatenation on the access point/bridge radio. Using concatenation, the access point/bridge combines multiple packets into one packet to reduce packet overhead and overall latency, which increases transmission efficiency.

Beginning in privileged EXEC mode, follow these steps to enable concatenation and set the maximum length of concatenation.

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.

	Command	Purpose
Step 3	concatenation <i>bytes</i>	(Optional) <i>Bytes</i> specifies a maximum size for concatenation packets in bytes. Enter a value from 1600 to 4000.
Step 4	end	Return to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Configuring the Radio Distance Setting

The **distance** command is active only when the access point/bridge is configured as a root bridge. Use the command to specify the distance from a root access point/bridge to the non-root access point/bridges with which it communicates. The distance setting adjusts the access point/bridge's time out values to account for the time required for radio signals to travel from access point/bridge to access point/bridge. If more than one non-root access point/bridge communicates with the root access point/bridge, enter the distance from the root access point/bridge to the non-root access point/bridge that is farthest away. Enter a value from 0 to 99 km. You do not need to adjust this setting on non-root access point/bridges.

In installation mode, the default distance setting is 99 km. In other modes, the default distance setting is 0 km.

Beginning in privileged EXEC mode, follow these steps to configure the access point/bridge distance setting:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.
Step 3	distance <i>kilometers</i>	Enter a distance setting from 0 to 99 km.
Step 4	end	Return to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Use the **no** form of the **distance** command to set the default distance.

Enabling and Disabling Reliable Multicast to Workgroup Bridges

The *Reliable multicast messages from the access point to workgroup bridges* setting limits reliable delivery of multicast messages to approximately 20 Cisco Aironet Workgroup Bridges that are associated to the access point. The default setting, **disabled**, reduces the reliability of multicast delivery to allow more workgroup bridges to associate to the access point.

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 maintain

a radio link 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.

Beginning in privileged EXEC mode, follow these steps to configure the encapsulation transformation method:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.
Step 3	infrastructure-client	Enable reliable multicast messages to workgroup bridges.
Step 4	end	Return to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Use the **no** form of the command to disable reliable multicast messages to workgroup bridges.

Enabling and Disabling Public Secure Packet Forwarding

Public Secure Packet Forwarding (PSPF) prevents client devices associated to an access point from inadvertently sharing files or communicating with other client devices associated to the access point. It provides Internet access to client devices without providing other capabilities of a LAN. This feature is useful for public wireless networks like those installed in airports or on college campuses.

**Note**

To prevent communication between clients associated to different access points, you must set up protected ports on the switch to which your access points are connected. See the [Configuring Protected Ports, page 6-18](#) for instructions on setting up protected ports.

To enable and disable PSPF using CLI commands on your access point, you use bridge groups. You can find a detailed explanation of bridge groups and instructions for implementing them in this document:

- *Cisco IOS Bridging and IBM Networking Configuration Guide, Release 12.2*. Click this link to browse to the Configuring Transparent Bridging chapter:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fibm_c/bcftb.htm

You can also enable and disable PSPF using the web-browser interface. The PSPF setting is on the Radio Settings pages.

PSPF is disabled by default. Beginning in privileged EXEC mode, follow these steps to enable PSPF:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.
Step 3	bridge-group <i>group</i> port-protected	Enable PSPF.
Step 4	end	Return to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Use the **no** form of the command to disable PSPF.

Configuring Protected Ports

To prevent communication between client devices associated to different access points on your wireless LAN, you must set up protected ports on the switch to which your access points are connected.

Beginning in privileged EXEC mode, follow these steps to define a port on your switch as a protected port:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface <i>interface-id</i>	Enter interface configuration mode, and enter the type and number of the switchport interface to configure, such as gigabitethernet0/1 .
Step 3	switchport protected	Configure the interface to be a protected port.
Step 4	end	Return to privileged EXEC mode.
Step 5	show interfaces <i>interface-id</i> switchport	Verify your entries.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To disable protected port, use the **no switchport protected** interface configuration command.

For detailed information on protected ports and port blocking, refer to the “Configuring Port-Based Traffic Control” chapter in the *Catalyst 3550 Multilayer Switch Software Configuration Guide, 12.1(12c)EA1*. Click this link to browse to that guide:

http://www.cisco.com/en/US/products/hw/switches/ps646/products_configuration_guide_book09186a008011591c.html

Enabling Short Slot Time

You can increase throughput on the 802.11g, 2.4-GHz radio by enabling short slot time. Reducing the slot time from the standard 20 microseconds to the 9-microsecond short slot time decreases the overall backoff, which increases throughput. Backoff, which is a multiple of the slot time, is the random length of time that a station waits before sending a packet on the LAN.

Many 802.11g radios support short slot time, but some do not. When you enable short slot time, the wireless device uses the short slot time only when all clients associated to the 802.11g, 2.4-GHz radio support short slot time.

In radio interface mode, enter this command to enable short slot time:

```
ap(config-if)# slot-time-short
```

Enter **no slot-time-short** to disable short slot time.

Configuring the Beacon Period and the DTIM

The beacon period is the amount of time between access point beacons in Kilomicroseconds. One Kµsec equals 1,024 microseconds. The Data Beacon Rate, 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.

For example, 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 wireless device sends a beacon containing a DTIM every 200 Kµsecs.

Beginning in privileged EXEC mode, follow these steps to configure the beacon period:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.
Step 3	beacon period <i>value</i>	Set the beacon period. Enter a value between 20 and 4000 Kµsecs.
Step 4	beacon dtim-period <i>value</i>	Set the DTIM. Enter a value between 1 and 100 Kilomicroseconds.
Step 5	end	Return to privileged EXEC mode.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Configure RTS Threshold and Retries

The RTS threshold determines the packet size at which the access point/bridge 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/bridge, or in areas where the clients are far apart and can detect only the access point/bridge and not each other. You can enter a setting ranging from 0 to 23472347 bytes.

**Note**

When concatenation is enabled, the RTS and fragment thresholds are set to 4000. Changing them to a lower value may degrade access point/bridge performance.

Maximum RTS Retries is the maximum number of times the access point/bridge issues an RTS before stopping the attempt to send the packet over the radio. Enter a value from 1 to 128.

The default RTS threshold is 2312, and the default maximum RTS retries setting is 32. Beginning in privileged EXEC mode, follow these steps to configure the RTS threshold and maximum RTS retries:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.
Step 3	rts threshold <i>value</i>	Set the RTS threshold. Enter a setting from 0 to 4000.
Step 4	rts retries <i>value</i>	Set the maximum RTS retries. Enter a setting from 1 to 128.
Step 5	end	Return to privileged EXEC mode.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Use the **no** form of the command to reset the RTS settings to defaults.

Configuring the Maximum Data Retries

The maximum data retries setting determines the number of attempts the access point/bridge makes to send a packet before giving up and dropping the packet.

The default setting is 32. Beginning in privileged EXEC mode, follow these steps to configure the maximum data retries:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.
Step 3	packet retries <i>value</i> drop-packet	Set the maximum data retries. Enter a setting from 1 to 128. Use the drop-packet command to maintain association and drop the packets when the maximum retry value is reached.
Step 4	end	Return to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Use the **no** form of the command to reset the setting to defaults.

Configuring the Fragmentation Threshold

The fragmentation threshold determines the size at which packets are fragmented (sent as several pieces instead of as one block). Use a low setting in areas where communication is poor or where there is a great deal of radio interference.



Note

When concatenation is enabled, the RTS and fragment thresholds are set to 4000. Changing them to a lower value may degrade access point/bridge performance.

The default setting is 2338 bytes. Beginning in privileged EXEC mode, follow these steps to configure the fragmentation threshold:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.
Step 3	fragment-threshold <i>value</i>	Set the fragmentation threshold. Enter a setting from 256 to 2346 bytes for the 2.4-GHz radio.
Step 4	end	Return to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Use the **no** form of the command to reset the setting to defaults.

Setting the Root Parent Timeout Value

Use the **parent timeout** command to define the amount of time that a non-root access point/bridge or workgroup bridge tries to associate with a parent access point. The command defines how long the access point/bridge or workgroup bridge attempts to associate with a parent in the parent list. If an association is not made within the timeout value, another acceptable parent is used. You set up the parent list using the **parent** command. With the timeout disabled, the parent must come from the parent list.

Beginning in privileged EXEC mode, follow these steps to configure the root parent timeout value:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.
Step 3	parent timeout <i>seconds</i>	The seconds value specifies the amount of time in seconds the non-root access point/bridge or workgroup bridge attempts to associate with a specified parent. Enter a value between 0 and 65535 seconds.
Step 4	end	Return to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Use the **no** form of the command to reset the setting to defaults.

Configuring the Root Parent MAC

Use the **parent** command to add a parent to a list of valid parent access points. The command adds a parent to the list of valid parent access points. You can use this command multiple times to define up to four valid parents. A repeater access point operates best when it is configured to associate with specific root access points that are connected to the wired LAN.

Beginning in privileged EXEC mode, follow these steps to configure the fragmentation threshold:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.
Step 3	parent 1-4 mac-address	The value 1-4 specifies the parent root access point number. mac-address specifies the MAC address of a parent access point (in xxxx.xxxx.xxxx format).
Step 4	end	Return to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Use the **no** form of the command to reset the setting to defaults.

Performing a Carrier Busy Test

You can perform a carrier busy test to check the radio activity on access point/bridge channels. During the carrier busy test, the access point/bridge drops all associations with wireless networking devices for around 4 seconds while it conducts the carrier test and then displays the test results.

In privileged EXEC mode, enter this command to perform a carrier busy test:

dot11 interface-number carrier busy

For *interface-number*, enter **dot11radio 0** to run the test on the 2.4-GHz radio, or enter **dot11radio 1** to run the test on the 5-GHz radio.

Use the **show dot11 carrier busy** command to re-display the carrier busy test results.



Configuring Multiple SSIDs

This chapter describes how to configure and manage multiple service set identifiers (SSIDs) on the access point/bridge. This chapter contains these sections:

- [Understanding Multiple SSIDs, page 7-2](#)
- [Configuring Multiple SSIDs, page 7-4](#)
- [Configuring Multiple Basic SSIDs, page 7-7](#)
- [Assigning IP Redirection for an SSID, page 7-10](#)
- [Including an SSID in an SSIDL IE, page 7-12](#)

Understanding Multiple SSIDs

The SSID is a unique identifier that wireless networking devices use to establish and maintain wireless connectivity. Multiple access points on a network or sub-network can use the same SSIDs. SSIDs are case sensitive and can contain up to 32 alphanumeric characters. Do not include spaces in your SSIDs.

You can configure up to 16 SSIDs on your access point/bridge and assign different configuration settings to each SSID. All the SSIDs are active at the same time; that is, client devices can associate to the access point/bridge using any of the SSIDs. These are the settings you can assign to each SSID:

- VLAN
- Client authentication method



Note For detailed information on client authentication types, see [Chapter 10, “Configuring Authentication Types.”](#)

- Maximum number of client associations using the SSID
- RADIUS accounting for traffic using the SSID
- Guest mode
- Repeater mode, including authentication username and password
- Redirection of packets received from client devices

If you want the access point/bridge to allow associations from client devices that do not specify an SSID in their configurations, you can set up a guest SSID. The access point/bridge includes the guest SSID in its beacon. The default SSID, *tsunami*, is set to guest mode. However, to keep your network secure, you should disable the guest mode SSID.

If your access point/bridge will be a repeater or will be a root access point that acts as a parent for a repeater, you can set up an SSID for use in repeater mode. You can assign an authentication username and password to the repeater-mode SSID to allow the repeater to authenticate to your network like a client device.

If your network uses VLANs, you can assign one SSID to a VLAN, and client devices using the SSID are grouped in that VLAN.

Effect of Software Versions on SSIDs

Cisco introduced global-mode SSID configuration in Cisco IOS Release 12.3(2)JA to simplify configuration of SSID parameters under multiple interfaces. Configuration of SSID parameters at the interface level was supported in Cisco IOS Release 12.3(2)JA release for backward compatibility, but configuration of SSID parameters at the interface level will be totally disabled in releases after Cisco IOS Release 12.3(4)JA. [Table 7-1](#) lists the SSID configuration methods supported in Cisco IOS Releases.

Table 7-1 SSID Configuration Methods Supported in Cisco IOS Releases

Cisco IOS Release	Supported SSID Configuration Method
12.2(15)JA	Interface-level only
12.3(2)JA	Both interface-level and global

Table 7-1 SSID Configuration Methods Supported in Cisco IOS Releases (continued)

Cisco IOS Release	Supported SSID Configuration Method
12.3(4)JA and 12.3(7)JA	Both interface-level and global; all SSIDs saved in global mode
post-12.3(4)JA	Global only

Cisco IOS Release 12.3(7)JA supports configuration of SSID parameters at the interface level on the CLI, but the SSIDs are stored in global mode. Storing all SSIDs in global mode ensures that the SSID configuration remains correct when you upgrade to release later than Cisco IOS Release 12.3(7)JA.

If you need to upgrade from Cisco IOS Release 12.3(2)JA or earlier to a release later than 12.3(4)JA, you should first upgrade to Cisco IOS Release 12.3(4)JA, save the configuration file, upgrade to the target release, and load the saved configuration file. This process ensures that your interface-level SSID configuration correctly translates to global mode. If you upgrade directly from a pre-12.3(4)JA release to a post-12.3(4)JA release, your interface-level SSID configuration is deleted.

If you downgrade the software version from Cisco IOS Release 12.3(7)JA, any SSIDs that you created become invalid. To avoid reconfiguring the SSIDs after a downgrade, save a copy of a configuration file in an earlier software version before you upgrade to Cisco IOS Release 12.3(7)JA; if you downgrade software versions from Cisco IOS Release 12.3(7)JA, load the saved configuration file after the downgrade.

Table 7-2 shows an example SSID configuration on an access point/bridge running Cisco IOS Release 12.2(15)JA and the configuration as it appears after upgrading to Cisco IOS Release 12.3(7)JA.

Table 7-2 Example: SSID Configuration Converted to Global Mode After Upgrade

SSID Configuration in 12.2(15)JA	SSID Configuration After Upgrade to 12.3(7)JA
<pre>interface dot11Radio 0 ssid engineering authentication open vlan 4 interface dot11Radio 1 ssid engineering authentication open vlan 5</pre>	<pre>dot11 ssid engineering authentication open vlan 5 ! interface dot11Radio 0 ssid engineering interface dot11Radio 1 ssid engineering</pre>

Note that the VLAN configuration under each interface is retained in the global SSID configuration.

**Note**

SSIDs, VLANs, and encryption schemes are mapped together on a one-to-one-to-one basis; one SSID can be mapped to one VLAN, and one VLAN can be mapped to one encryption scheme. When using a global SSID configuration, you cannot configure one SSID with two different encryption schemes. For example, you cannot apply SSID *north* with TKIP on interface dot11 0 and also apply SSID *north* with WEP128 on interface dot11 1.

Configuring Multiple SSIDs

These sections contain configuration information for multiple SSIDs:

- [Default SSID Configuration, page 7-4](#)
- [Creating an SSID Globally, page 7-4](#)
- [Using a RADIUS Server to Restrict SSIDs, page 7-6](#)



Note

In Cisco IOS Release 12.3(4)JA and later, you configure SSIDs globally and then apply them to a specific radio interface. Follow the instructions in the [“Creating an SSID Globally” section on page 7-4](#) to configure SSIDs globally.

Default SSID Configuration

In Cisco IOS Release 12.3(7)JA there is no default SSID.

Creating an SSID Globally

In Cisco IOS Releases 12.3(2)JA and later, you can configure SSIDs globally or for a specific radio interface. When you use the **dot11 ssid** global configuration command to create an SSID, you can use the **ssid** configuration interface command to assign the SSID to a specific interface.

When an SSID has been created in global configuration mode, the **ssid** configuration interface command attaches the SSID to the interface but does not enter **ssid** configuration mode. However, if the SSID has not been created in global configuration mode, the **ssid** command puts the CLI into SSID configuration mode for the new SSID.



Note

SSIDs created in Cisco IOS Releases 12.3(7)JA and later become invalid if you downgrade the software version to an earlier release.

Beginning in privileged EXEC mode, follow these steps to create an SSID globally. After you create an SSID, you can assign it to specific radio interfaces.

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	dot11 ssid <i>ssid-string</i>	Create an SSID and enter SSID configuration mode for the new SSID. The SSID can consist of up to 32 alphanumeric characters. SSIDs are case sensitive. Note +,], ?, \$, TAB, and trailing spaces are invalid characters for SSIDs.
Step 3	authentication client username <i>username</i> password <i>password</i>	(Optional) Set an authentication username and password that the access point/bridge uses to authenticate to the network when in repeater mode. Set the username and password on the SSID that the repeater access point uses to associate to a root access point, or with another repeater.

	Command	Purpose
Step 4	accounting <i>list-name</i>	(Optional) Enable RADIUS accounting for this SSID. For <i>list-name</i> , specify the accounting method list. Click this link for more information on method lists: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fsaaa/scfacct.htm#xtocid2
Step 5	vlan <i>vlan-id</i>	(Optional) Assign the SSID to a VLAN on your network. Client devices that associate using the SSID are grouped into this VLAN. You can assign only one SSID to a VLAN.
Step 6	guest-mode	(Optional) Designate the SSID as your access point/bridge's guest-mode SSID. The access point/bridge includes the SSID in its beacon and allows associations from client devices that do not specify an SSID.
Step 7	infrastructure-ssid [optional]	(Optional) Designate the SSID as the SSID that other access points and workgroup bridges use to associate to this access point. If you do not designate an SSID as the infrastructure SSID, infrastructure devices can associate to the access point using any SSID. If you designate an SSID as the infrastructure SSID, infrastructure devices must associate to the access point using that SSID unless you also enter the optional keyword.
Step 8	interface dot11radio 0	Enter interface configuration mode for the radio interface to which you want to assign the SSID.
Step 9	ssid <i>ssid-string</i>	Assign the global SSID that you created in Step 2 to the radio interface.
Step 10	end	Return to privileged EXEC mode.
Step 11	copy running-config startup-config	(Optional) Save your entries in the configuration file.

**Note**

You use the **ssid** command's authentication options to configure an authentication type for each SSID. See [Chapter 10, "Configuring Authentication Types,"](#) for instructions on configuring authentication types.

Use the **no** form of the command to disable the SSID or to disable SSID features.

This example shows how to:

- Name an SSID
- Configure the SSID for RADIUS accounting
- Set the maximum number of client devices that can associate using this SSID to 15
- Assign the SSID to a VLAN
- Assign the SSID to a radio interface

```
AP# configure terminal
AP(config)# dot11 ssid batman
AP(config-ssid)# accounting accounting-method-list
AP(config-ssid)# max-associations 15
AP(config-ssid)# vlan 3762
AP(config-ssid)# exit
AP(config)# interface dot11radio 0
AP(config-if)# ssid batman
```

Viewing SSIDs Configured Globally

Use this command to view configuration details for SSIDs that are configured globally:

```
AP# show running-config ssid ssid-string
```

Using Spaces in SSIDs

In Cisco IOS Release 12.3(7)JA, You can include spaces in an SSID, but trailing spaces (spaces at the end of an SSID) are invalid. However, any SSIDs created in previous versions having trailing spaces are recognized. Trailing spaces make it appear that you have identical SSIDs configured on the same access point. If you think identical SSIDs are on the access point, use the **show dot11 associations** privileged EXEC command to check any SSIDs created in a previous release for trailing spaces.

For example, this sample output from a **show configuration** privileged EXEC command does not show spaces in SSIDs:

```
ssid buffalo
  vlan 77
  authentication open

ssid buffalo
  vlan 17
  authentication open

ssid buffalo
  vlan 7
  authentication open
```

However, this sample output from a **show dot11 associations** privileged EXEC command shows the spaces in the SSIDs:

```
SSID [buffalo] :
SSID [buffalo ] :
SSID [buffalo ] :
```

Using a RADIUS Server to Restrict SSIDs

To prevent client devices from associating to the access point/bridge using an unauthorized SSID, you can create a list of authorized SSIDs that clients must use on your RADIUS authentication server.

The SSID authorization process consists of these steps:

1. A client device associates to the access point/bridge using any SSID configured on the access point/bridge.
2. The client begins RADIUS authentication.
3. The RADIUS server returns a list of SSIDs that the client is allowed to use. The access point/bridge checks the list for a match of the SSID used by the client. There are three possible outcomes:
 - a. If the SSID that the client used to associate to the access point/bridge matches an entry in the allowed list returned by the RADIUS server, the client is allowed network access after completing all authentication requirements.

- b. If the access point/bridge does not find a match for the client in the allowed list of SSIDs, the access point/bridge disassociates the client.
- c. If the RADIUS server does not return any SSIDs (no list) for the client, then the administrator has not configured the list, and the client is allowed to associate and attempt to authenticate.

The allowed list of SSIDs from the RADIUS server are in the form of Cisco VSAs. The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific information between the access point/bridge and the RADIUS server by using the vendor-specific attribute (attribute 26). Vendor-specific attributes (VSAs) allow vendors to support their own extended attributes not suitable for general use. The Cisco RADIUS implementation supports one vendor-specific option by using the format recommended in the specification. Cisco's vendor-ID is 9, and the supported option has vendor-type 1, which is named *cisco-avpair*. The Radius server is allowed to have zero or more SSID VSAs per client.

In this example, the following AV pair adds the SSID *batman* to the list of allowed SSIDs for a user:

```
cisco-avpair= "ssid=batman"
```

For instructions on configuring the access point/bridge to recognize and use VSAs, see Chapter 12 of the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*.

Configuring Multiple Basic SSIDs

Access point 802.11g radios now support up to 8 basic SSIDs (BSSIDs), which are similar to MAC addresses. You use multiple BSSIDs to assign a unique DTIM setting for each SSID and to broadcast more than one SSID in beacons. A large DTIM value increases battery life for power-save client devices that use an SSID, and broadcasting multiple SSIDs makes your wireless LAN more accessible to guests.



Note

Devices on your wireless LAN that are configured to associate to a specific access point based on the access point MAC address (for example, client devices, repeaters, hot standby units, or workgroup bridges) might lose their association when you add or delete a multiple BSSID. When you add or delete a multiple BSSID, check the association status of devices configured to associate to a specific access point. If necessary, reconfigure the disassociated device to use the BSSID's new MAC address.

Requirements for Configuring Multiple BSSIDs

To configure multiple BSSIDs, your access point/bridge must meet these minimum requirements:

- VLANs must be configured
- The access point/bridge must run Cisco IOS Release 12.3(4)JA or later
- The access point/bridge must contain an 802.11g radio that supports multiple BSSIDs

To determine whether a radio supports multiple basic SSIDs, enter the **show controllers radio_interface** command. The radio supports multiple basic SSIDs if the results include this line:

```
Number of supported simultaneous BSSID on radio_interface: 8
```

Guidelines for Using Multiple BSSIDs

Keep these guidelines in mind when configuring multiple BSSIDs:

- RADIUS-assigned VLANs are not supported when you enable multiple BSSIDs.
- When you enable BSSIDs, the access point/bridge automatically maps a BSSID to each SSID. You cannot manually map a BSSID to a specific SSID.
- When multiple BSSIDs are enabled on the access point/bridge, the SSIDL IE does not contain a list of SSIDs; it contains only extended capabilities.
- Any Wi-Fi certified client device can associate to an access point/bridge using multiple BSSIDs.
- You can enable multiple BSSIDs on access point/bridges that participate in WDS.

Configuring Multiple BSSIDs

Follow these steps to configure multiple BSSIDs:

-
- Step 1** Browse to the Global SSID Manager page on the access point GUI. (If you use the CLI instead of the GUI, refer to the CLI commands listed in the [CLI Configuration Example](#) at the end of this section.) [Figure 7-1](#) shows the top portion of the Global SSID Manager page.

Figure 7-1 Global SSID Manager Page

Hostname BR1310G BR1310G uptime is 3 days, 11 hours, 6 minutes

Security: Global SSID Manager

SSID Properties

Current SSID List

< NEW >	SSID:	
1310test	VLAN:	< NONE > Define VLANs
	Interface:	☐ Radio0-802.11G
	Network ID:	(0-4096)

Authentication Settings

Methods Accepted:

☒ Open Authentication:

☐ Shared Authentication:

- Step 2** Enter the SSID name in the **SSID** field.
- Step 3** Use the **VLAN** drop-down menu to select the VLAN to which the SSID is assigned.
- Step 4** Select the radio interfaces on which the SSID is enabled. The SSID remains inactive until you enable it for a radio interface.
- Step 5** Enter a Network ID for the SSID in the **Network ID** field.
- Step 6** Assign authentication, authenticated key management, and accounting settings to the SSID in the Authentication Settings, Authenticated Key Management, and Accounting Settings sections of the page. BSSIDs support all the authentication types that are supported on SSIDs.
- Step 7** (Optional) In the Multiple BSSID Beacon Settings section, select the **Set SSID as Guest Mode** check box to include the SSID in beacons.
- Step 8** (Optional) To increase the battery life for power-save clients that use this SSID, select the **Set Data Beacon Rate (DTIM)** check box and enter a beacon rate for the SSID. The beacon rate determines how often the access point sends a beacon containing a Delivery Traffic Indicator Message (DTIM).

When client devices receive a beacon that contains a DTIM, they normally wake up to check for pending packets. Longer intervals between DTIMs let clients sleep longer and preserve power. Conversely, shorter DTIM periods reduce the delay in receiving packets but use more battery power because clients wake up more often.

The default beacon rate is 2, which means that every other beacon contains a DTIM. Enter a beacon rate between 1 and 100.

**Note**

Increasing the DTIM period count delays the delivery of multicast packets. Because multicast packets are buffered, large DTIM period counts can cause a buffer overflow.

- Step 9** In the Guest Mode/Infrastructure SSID Settings section, select **Multiple BSSID**.
- Step 10** Click **Apply**.

CLI Configuration Example

This example shows the CLI commands that you use to enable multiple BSSIDs on a radio interface, create an SSID called *visitor*, designate the SSID as a BSSID, specify that the BSSID is included in beacons, set a DTIM period for the BSSID, and assign the SSID *visitor* to the radio interface:

```
ap(config)# interface d0
ap(config-if)# mbssid
ap(config-if)# exit
ap(config)# dot11 ssid visitor
ap(config-ssid)# mbssid guest-mode dtim-period 75
ap(config-ssid)# exit
ap(config)# interface d0
ap(config-if)# ssid visitor
```

You can also use the **dot11 mbssid** global configuration command to simultaneously enable multiple BSSIDs on all radio interfaces that support multiple BSSIDs.

Displaying Configured BSSIDs

Use the **show dot11 bssid** privileged EXEC command to display the relationship between SSIDs and BSSIDs or MAC addresses. This example shows the command output:

```
ap#show dot11 bssid
Interface      BSSID           Guest  SSID
Dot11Radio1    0011.2161.b7c0  Yes    atlantic
Dot11Radio0    0005.9a3e.7c0f  Yes    WPA2-TLS-g
```

Assigning IP Redirection for an SSID

When you configure IP redirection for an SSID, the access point/bridge redirects all packets sent from client devices associated to that SSID to a specific IP address. IP redirection is used mainly on wireless LANs serving handheld devices that use a central software application and are statically configured to communicate with a specific IP address. For example, the wireless LAN administrator at a retail store or warehouse might configure IP redirection for its bar code scanners, which all use the same scanner application and all send data to the same IP address.

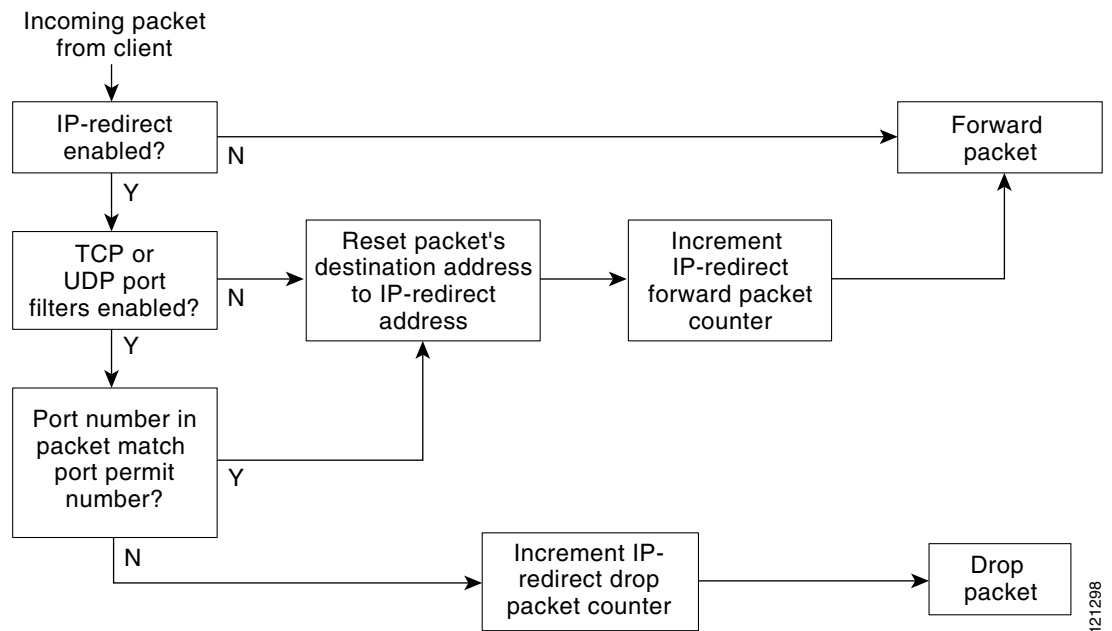
You can redirect all packets from client devices associated using an SSID or redirect only packets directed to specific TCP or UDP ports (as defined in an access control list). When you configure the access point/bridge to redirect only packets addressed to specific ports, the access point/bridge redirects those packets from clients using the SSID and drops all other packets from clients using the SSID.



Note

When you perform a ping test from the access point/bridge to a client device that is associated using an IP-redirect SSID, the response packets from the client are redirected to the specified IP address and are not received by the access point/bridge.

Figure 7-2 shows the processing flow that occurs when the access point/bridge receives client packets from clients associated using an IP-redirect SSID.

Figure 7-2 Processing Flow for IP Redirection

12/298

Guidelines for Using IP Redirection

Keep these guidelines in mind when using IP redirection:

- The access point/bridge does not redirect broadcast, unicast, or multicast BOOTP/DHCP packets received from client devices.
- Existing ACL filters for incoming packets take precedence over IP redirection.

Configuring IP Redirection

Beginning in privileged EXEC mode, follow these steps to configure IP redirection for an SSID:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.
Step 3	ssid ssid-string	Enter configuration mode for a specific SSID.

	Command	Purpose
Step 4	ip redirection host <i>ip-address</i>	Enter IP redirect configuration mode for the IP address. Enter the IP address with decimals, as in this example: 10.91.104.92 If you do not specify an access control list (ACL) which defines TCP or UDP ports for redirection, the access point/bridge redirects all packets that it receives from client devices.
Step 5	ip redirection host <i>ip-address</i> access-group <i>acl</i> in	(Optional) Specify an ACL to apply to the redirection of packets. Only packets sent to the specific UDP or TCP ports defined in the ACL are redirected. The access point/bridge discards all received packets that do not match the settings defined in the ACL. The in parameter specifies that the ACL is applied to the access point/bridge's incoming interface.

This example shows how to configure IP redirection for an SSID without applying an ACL. The access point/bridge redirects all packets that it receives from client devices associated to the SSID *batman*:

```
ap# configure terminal
ap(config)# interface dot11radio 0
ap(config-if)# ssid batman
ap(config-if-ssid)# ip redirection host 10.91.104.91
ap(config-if-ssid-redirect)# end
```

This example shows how to configure IP redirection only for packets sent to the specific TCP and UDP ports specified in an ACL. When the access point receives packets from client devices associated using the SSID *robin*, it redirects packets sent to the specified ports and discards all other packets:

```
ap# configure terminal
ap(config)# interface dot11radio 0
ap(config-if)# ssid robin
ap(config-if-ssid)# ip redirection host 10.91.104.91 access-group redirect-acl in
ap(config-if-ssid)# end
```

Including an SSID in an SSIDL IE

The access point/bridge beacon can advertise only one broadcast SSID. However, you can use SSIDL information elements (SSIDL IEs) in the access point/bridge beacon to alert client devices of additional SSIDs on the access point/bridge. When you designate an SSID to be included in an SSIDL IE, client devices detect that the SSID is available, and they also detect the security settings required to associate using that SSID.



Note

When multiple BSSIDs are enabled on the access point/bridge, the SSIDL IE does not contain a list of SSIDs; it contains only extended capabilities.

Beginning in privileged EXEC mode, follow these steps to include an SSID in an SSIDL IE:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.

	Command	Purpose
Step 3	ssid <i>ssid-string</i>	Enter configuration mode for a specific SSID.
Step 4	information-element ssidl [advertisement] [wps]	Include an SSIDL IE in the access point/bridge beacon that advertises the access point/bridge's extended capabilities, such as 802.1x and support for Microsoft Wireless Provisioning Services (WPS). Use the advertisement option to include the SSID name and capabilities in the SSIDL IE. Use the wps option to set the WPS capability flag in the SSIDL IE.

Use the **no** form of the command to disable SSIDL IEs.



Configuring Spanning Tree Protocol

This chapter describes how to configure Spanning Tree Protocol (STP) on your access point/bridge. This chapter contains these sections:

- [Understanding Spanning Tree Protocol, page 8-2](#)
- [Configuring STP Features, page 8-8](#)
- [Displaying Spanning-Tree Status, page 8-14](#)



Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Cisco IOS Command Reference for Access Points and Bridges* for this release.

Understanding Spanning Tree Protocol

This section describes how spanning-tree features work. It includes this information:

- [STP Overview, page 8-2](#)
- [Access Point/Bridge Protocol Data Units, page 8-3](#)
- [Election of the Spanning-Tree Root, page 8-4](#)
- [Spanning-Tree Timers, page 8-5](#)
- [Creating the Spanning-Tree Topology, page 8-5](#)
- [Spanning-Tree Interface States, page 8-6](#)

STP Overview

STP is a Layer 2 link management protocol that provides path redundancy while preventing loops in the network. For a Layer 2 Ethernet network to function properly, only one active path can exist between any two stations. Spanning-tree operation is transparent to end stations, which cannot detect whether they are connected to a single LAN segment or to a LAN of multiple segments.

When you create fault-tolerant internetworks, you must have a loop-free path between all nodes in a network. The spanning-tree algorithm calculates the best loop-free path throughout a Layer 2 network. Infrastructure devices such as wireless access point/bridges and switches send and receive spanning-tree frames, called bridge protocol data units (BPDUs), at regular intervals. The devices do not forward these frames but use them to construct a loop-free path.

Multiple active paths among end stations cause loops in the network. If a loop exists in the network, end stations might receive duplicate messages. Infrastructure devices might also learn end-station MAC addresses on multiple Layer 2 interfaces. These conditions result in an unstable network.

STP defines a tree with a root bridge and a loop-free path from the root to all infrastructure devices in the Layer 2 network.



Note

STP discussions use the term *root* to describe two concepts: the bridge on the network that serves as a central point in the spanning tree is called the *root bridge*, and the port on each bridge that provides the most efficient path to the root bridge is called the *root port*. These meanings are separate from the Role in radio network setting that includes root and non-root options. A bridge whose Role in radio network setting is Root Bridge does not necessarily become the root bridge in the spanning tree. In this chapter, the root bridge in the spanning tree is called the *spanning-tree root*.

STP forces redundant data paths into a standby (blocked) state. If a network segment in the spanning tree fails and a redundant path exists, the spanning-tree algorithm recalculates the spanning-tree topology and activates the standby path.

When two interfaces on a bridge are part of a loop, the spanning-tree port priority and path cost settings determine which interface is put in the forwarding state and which is put in the blocking state. The port priority value represents the location of an interface in the network topology and how well it is located to pass traffic. The path cost value represents media speed.

The access point/bridge supports both per-VLAN spanning tree (PVST) and a single 802.1q spanning tree without VLANs. The access point/bridge cannot run 802.1s MST or 802.1d Common Spanning Tree, which maps multiple VLANs into a one-instance spanning tree.

The access point/bridge maintains a separate spanning-tree instance for each active VLAN configured on it. A bridge ID, consisting of the bridge priority and the access point/bridge MAC address, is associated with each instance. For each VLAN, the access point/bridge with the lowest access point/bridge ID becomes the spanning-tree root for that VLAN.

350 Series Bridge Interoperability

Cisco Aironet 1300 and 350 Series Bridges are interoperable when STP is enabled and no VLANs are configured. This configuration is the only one available for the following reasons:

- When STP is disabled, the 350 series bridge acts as a 350 series access point and disallows association of non-root bridges, including non-root 350 and 1300 series bridges.
- The 350 series bridge supports only a single instance of STP in both non-VLAN and VLAN configurations, while the 1300 series bridge has a single instance of STP in non-VLAN configurations and multiple instances of STP in VLAN configurations.
- Incompatibilities between single and multiple instances of STP can cause inconsistent blocking of traffic when VLANs are configured. When the native VLAN is blocked, you can experience bridge flapping.

Therefore, the best configuration for STP interoperability is when the 350 and 1300 series access point/bridges STP feature is enabled and VLANs are not configured.



Note

When the 350 and 1300 series access point/bridges are configured as workgroup bridges, they can operate with STP disabled and allow for associations with access points. However, this configuration is not technically a bridge-to-bridge scenario.

Access Point/Bridge Protocol Data Units

The stable, active spanning-tree topology of your network is determined by these elements:

- The unique access point/bridge ID (wireless access point/bridge priority and MAC address) associated with each VLAN on each wireless access point/bridge
- The spanning-tree path cost to the spanning-tree root
- The port identifier (port priority and MAC address) associated with each Layer 2 interface

When the access point/bridges in a network are powered up, each access point/bridge functions as the STP root. The access point/bridges send configuration BPDUs through the Ethernet and radio ports. The BPDUs communicate and compute the spanning-tree topology. Each configuration BPDU contains this information:

- The unique access point/bridge ID of the wireless access point/bridge that the sending access point/bridge identifies as the spanning-tree root
- The spanning-tree path cost to the root
- The access point/bridge ID of the sending access point/bridge
- Message age
- The identifier of the sending interface
- Values for the hello, forward delay, and max-age protocol timers

When an access point/bridge receives a configuration BPDU that contains *superior* information (lower access point/bridge ID, lower path cost, and so forth), it stores the information for that port. If this BPDU is received on the root port of the access point/bridge, the access point/bridge also forwards it with an updated message to all attached LANs for which it is the designated access point/bridge.

If an access point/bridge receives a configuration BPDU that contains *inferior* information to that currently stored for that port, it discards the BPDU. If the access point/bridge is a designated access point/bridge for the LAN from which the inferior BPDU was received, it sends that LAN a BPDU containing the up-to-date information stored for that port. In this way, inferior information is discarded, and superior information is propagated on the network.

A BPDU exchange results in these actions:

- One access point/bridge is elected as the spanning-tree root.
- A root port is selected for each access point/bridge (except the spanning-tree root). This port provides the best path (lowest cost) when the access point/bridge forwards packets to the spanning-tree root.
- The shortest distance to the spanning-tree root is calculated for each access point/bridge based on the path cost.
- A designated access point/bridge for each LAN segment is selected. The designated access point/bridge incurs the lowest path cost when forwarding packets from that LAN to the spanning-tree root. The port through which the designated access point/bridge is attached to the LAN is called the *designated port*.
- Interfaces included in the spanning-tree instance are selected. Root ports and designated ports are put in the forwarding state.
- All interfaces not included in the spanning tree are blocked.

Election of the Spanning-Tree Root

All access point/bridges in the Layer 2 network participating in STP gather information about other access point/bridges in the network through an exchange of BPDU data messages. This exchange of messages results in these actions:

- The election of a unique spanning-tree root for each spanning-tree instance
- The election of a designated access point/bridge for every LAN segment
- The removal of loops in the network by blocking Layer 2 interfaces connected to redundant links

For each VLAN, the access point/bridge with the highest access point/bridge priority (the lowest numerical priority value) is elected as the spanning-tree root. If all access point/bridges are configured with the default priority (32768), the access point/bridge with the lowest MAC address in the VLAN becomes the spanning-tree root. The access point/bridge priority value occupies the most significant bits of the access point/bridge ID.

When you change the access point/bridge priority value, you change the probability that the access point/bridge will be elected as the root access point/bridge. Configuring a higher value decreases the probability; a lower value increases the probability.

The spanning-tree root is the logical center of the spanning-tree topology. All paths that are not needed to reach the spanning-tree root from anywhere in the network are placed in the spanning-tree blocking mode.

BPDUs contain information about the sending access point/bridge and its ports, including access point/bridge and MAC addresses, access point/bridge priority, port priority, and path cost. STP uses this information to elect the spanning-tree root and root port for the network and the root port and designated port for each LAN segment.

Spanning-Tree Timers

Table 8-1 describes the timers that affect the entire spanning-tree performance.

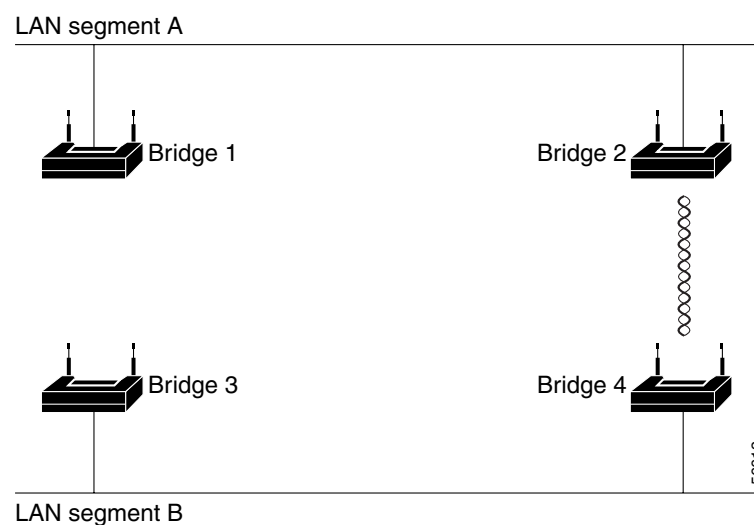
Table 8-1 Spanning-Tree Timers

Variable	Description
Hello timer	Determines how often the access point/bridge broadcasts hello messages to other access point/bridges.
Forward-delay timer	Determines how long each of the listening and learning states last before the interface begins forwarding.
Maximum-age timer	Determines the amount of time the access point/bridge stores protocol information received on an interface.

Creating the Spanning-Tree Topology

In Figure 8-1, bridge 4 is elected as the spanning-tree root because the priority of all the access point/bridges is set to the default (32768) and bridge 4 has the lowest MAC address. However, because of traffic patterns, number of forwarding interfaces, or link types, bridge 4 might not be the ideal spanning-tree root. By increasing the priority (lowering the numerical value) of the ideal bridge so that it becomes the spanning-tree root, you force a spanning-tree recalculation to form a new topology with the ideal bridge as the spanning-tree root.

Figure 8-1 Spanning-Tree Topology



Spanning-Tree Interface States

Propagation delays can occur when protocol information passes through a wireless LAN. As a result, topology changes can take place at different times and at different places in the network. When an interface transitions directly from nonparticipation in the spanning-tree topology to the forwarding state, it can create temporary data loops. Interfaces must wait for new topology information to propagate through the LAN before starting to forward frames. They must allow the frame lifetime to expire for forwarded frames that have used the old topology.

Each interface on a access point/bridge using spanning tree exists in one of these states:

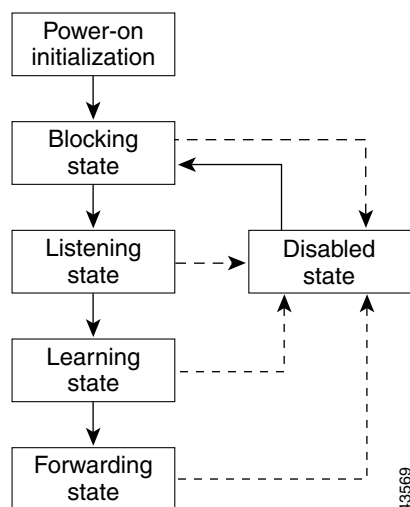
- Blocking—The interface does not participate in frame forwarding.
- Listening—The first transitional state after the blocking state when the spanning tree determines that the interface should participate in frame forwarding.
- Learning—The interface prepares to participate in frame forwarding.
- Forwarding—The interface forwards frames.
- Disabled—The interface is not participating in spanning tree because of a shutdown port, no link on the port, or no spanning-tree instance running on the port.

An interface moves through these states:

- From initialization to blocking
- From blocking to listening or to disabled
- From listening to learning or to disabled
- From learning to forwarding or to disabled
- From forwarding to disabled

Figure 8-2 illustrates how an interface moves through the states.

Figure 8-2 Spanning-Tree Interface States



When you enable STP on the access point/bridge, the Ethernet and radio interfaces go through the blocking state and the transitory states of listening and learning. Spanning tree stabilizes each interface at the forwarding or blocking state.

When the spanning-tree algorithm places a Layer 2 interface in the forwarding state, this process occurs:

1. The interface is in the listening state while spanning tree waits for protocol information to transition the interface to the blocking state.
2. While spanning tree waits the forward-delay timer to expire, it moves the interface to the learning state and resets the forward-delay timer.
3. In the learning state, the interface continues to block frame forwarding as the access point/bridge learns end-station location information for the forwarding database.
4. When the forward-delay timer expires, spanning tree moves the interface to the forwarding state, where both learning and frame forwarding are enabled.

Blocking State

An interface in the blocking state does not participate in frame forwarding. After initialization, a BPDU is sent to the access point/bridge's Ethernet and radio ports. A access point/bridge initially functions as the spanning-tree root until it exchanges BPDUs with other access point/bridges. This exchange establishes which access point/bridge in the network is the spanning-tree root. If there is only one access point/bridge in the network, no exchange occurs, the forward-delay timer expires, and the interfaces move to the listening state. An interface always enters the blocking state when you enable STP.

An interface in the blocking state performs as follows:

- Discards frames received on the port
- Does not learn addresses
- Receives BPDUs



Note

If a access point/bridge port is blocked, some broadcast or multicast packets can reach a forwarding port on the access point/bridge and cause the bridging logic to switch the blocked port into listening state momentarily before the packets are dropped at the blocked port.

Listening State

The listening state is the first state an interface enters after the blocking state. The interface enters this state when STP determines that the interface should participate in frame forwarding.

An interface in the listening state performs as follows:

- Discards frames received on the port
- Does not learn addresses
- Receives BPDUs

Learning State

An interface in the learning state prepares to participate in frame forwarding. The interface enters the learning state from the listening state.

An interface in the learning state performs as follows:

- Discards frames received on the port
- Learns addresses
- Receives BPDUs

Forwarding State

An interface in the forwarding state forwards frames. The interface enters the forwarding state from the learning state.

An interface in the forwarding state performs as follows:

- Receives and forwards frames received on the port
- Learns addresses
- Receives BPDUs

Disabled State

An interface in the disabled state does not participate in frame forwarding or in the spanning tree. An interface in the disabled state is nonoperational.

A disabled interface performs as follows:

- Discards frames received on the port
- Does not learn addresses
- Does not receive BPDUs

Configuring STP Features

You complete three major steps to configure STP on the access point/bridge:

1. If necessary, assign interfaces and sub-interfaces to bridge groups
2. Enable STP for each bridge group
3. Set the STP priority for each bridge group

These sections include spanning-tree configuration information:

- [Default STP Configuration, page 8-9](#)
- [Configuring STP Settings, page 8-9](#)
- [STP Configuration Examples, page 8-10](#)

Default STP Configuration

STP is disabled by default. [Table 8-2](#) lists the default STP settings when you enable STP.

Table 8-2 *Default STP Values When STP is Enabled*

Setting	Default Value
Bridge priority	32768
Bridge max age	20
Bridge hello time	2
Bridge forward delay	15
Ethernet port path cost	19
Ethernet port priority	128
Radio port path cost	33
Radio port priority	128

The radio and Ethernet interfaces and the native VLAN on the access point/bridge are assigned to bridge group 1 by default. When you enable STP and assign a priority on bridge group 1, STP is enabled on the radio and Ethernet interfaces and on the primary VLAN, and those interfaces adopt the priority assigned to bridge group 1. You can create bridge groups for sub-interfaces and assign different STP settings to those bridge groups.

Configuring STP Settings

Beginning in privileged EXEC mode, follow these steps to configure STP on the access point/bridge:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface { dot11radio number fastethernet number }	Enter interface configuration mode for radio or Ethernet interfaces or sub-interfaces.
Step 3	bridge-group number	Assign the interface to a bridge group. You can number your bridge groups from 1 to 255.
Step 4	no bridge-group number spanning-disabled	Counteract the command that automatically disables STP for a bridge group. STP is enabled on the interface when you enter the bridge n protocol ieee command.
Step 5	exit	Return to global configuration mode.
Step 6	bridge number protocol ieee	Enable STP for the bridge group. You must enable STP on each bridge group that you create with bridge-group commands.

	Command	Purpose
Step 7	bridge <i>number</i> priority <i>priority</i>	(Optional) Assign a priority to a bridge group. The lower the priority, the more likely it is that the bridge becomes the spanning-tree root.
Step 8	end	Return to privileged EXEC mode.
Step 9	show spanning-tree bridge	Verify your entries.
Step 10	copy running-config startup-config	(Optional) Save your entries in the configuration file.

STP Configuration Examples

These configuration examples show how to enable STP on root and non-root access point/bridges with and without VLANs:

- [Root Bridge Without VLANs, page 8-10](#)
- [Non-Root Bridge Without VLANs, page 8-11](#)
- [Root Bridge with VLANs, page 8-12](#)
- [Non-Root Bridge with VLANs, page 8-13](#)

Root Bridge Without VLANs

This example shows the configuration of a root bridge with no VLANs configured and with STP enabled:

```
hostname master-bridge-south
ip subnet-zero
!
bridge irb
!
interface Dot11Radio0
no ip address
no ip route-cache
!
ssid tsunami
authentication open
guest-mode
!
speed basic-6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
rts threshold 2312
station-role root
no cdp enable
infrastructure-client
bridge-group 1
!
interface FastEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
bridge-group 1
!
interface BVI1
ip address 1.4.64.23 255.255.0.0
no ip route-cache
!
```

```
ip default-gateway 1.4.0.1
bridge 1 protocol ieee
bridge 1 route ip
bridge 1 priority 9000
!
line con 0
exec-timeout 0 0
line vty 0 4
login
line vty 5 15
login
!
end
```

Non-Root Bridge Without VLANs

This example shows the configuration of a non-root bridge with no VLANs configured with STP enabled:

```
hostname client-bridge-north
ip subnet-zero
!
bridge irb
!
interface Dot11Radio0
no ip address
no ip route-cache
!
ssid tsunami
authentication open
guest-mode
!
speed basic-6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
rts threshold 2312
station-role non-root
no cdp enable
bridge-group 1
!
interface FastEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
bridge-group 1 path-cost 40
!
interface BVI1
ip address 1.4.64.24 255.255.0.0
no ip route-cache
!
bridge 1 protocol ieee
bridge 1 route ip
bridge 1 priority 10000
!
line con 0
line vty 0 4
login
line vty 5 15
login
!
end
```

Root Bridge with VLANs

This example shows the configuration of a root bridge with VLANs configured with STP enabled:

```
hostname master-bridge-hq
!
ip subnet-zero
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
bridge irb
!
interface Dot11Radio0
no ip address
no ip route-cache
!
ssid vlan1
vlan 1
infrastructure-ssid
authentication open
!
speed basic-6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
rts threshold 2312
station-role root
no cdp enable
infrastructure-client
!
interface Dot11Radio0.1
encapsulation dot1Q 1 native
no ip route-cache
no cdp enable
bridge-group 1
!
interface Dot11Radio0.2
encapsulation dot1Q 2
no ip route-cache
no cdp enable
bridge-group 2
!
interface Dot11Radio0.3
encapsulation dot1Q 3
no ip route-cache
bridge-group 3
bridge-group 3 path-cost 500
!
interface FastEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
!
interface FastEthernet0.1
encapsulation dot1Q 1 native
no ip route-cache
bridge-group 1
!
interface FastEthernet0.2
encapsulation dot1Q 2
no ip route-cache
```



```
bridge-group 2
!
interface FastEthernet0.3
encapsulation dot1Q 3
no ip route-cache
bridge-group 3
!
interface BVI1
ip address 1.4.64.23 255.255.0.0
no ip route-cache
!
ip default-gateway 1.4.0.1
bridge 1 protocol ieee
bridge 1 route ip
bridge 1 priority 9000
bridge 2 protocol ieee
bridge 2 priority 10000
bridge 3 protocol ieee
bridge 3 priority 3100
!
line con 0
exec-timeout 0 0
line vty 5 15
!
end
```

Non-Root Bridge with VLANs

This example shows the configuration of a non-root bridge with VLANs configured with STP enabled:

```
hostname client-bridge-remote
!
ip subnet-zero
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
bridge irb
!
interface Dot11Radio0
no ip address
no ip route-cache
!
ssid vlan1
vlan 1
authentication open
infrastructure-ssid
!
speed basic-6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
rts threshold 2312
station-role non-root
no cdp enable
!
interface Dot11Radio0.1
encapsulation dot1Q 1 native
no ip route-cache
no cdp enable
bridge-group 1
!
interface Dot11Radio0.2
encapsulation dot1Q 2
no ip route-cache
```

```

no cdp enable
bridge-group 2
!
interface Dot11Radio0.3
encapsulation dot1Q 3
no ip route-cache
no cdp enable
bridge-group 3
!
interface FastEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
!
interface FastEthernet0.1
encapsulation dot1Q 1 native
no ip route-cache
bridge-group 1
!
interface FastEthernet0.2
encapsulation dot1Q 2
no ip route-cache
bridge-group 2
!
interface FastEthernet0.3
encapsulation dot1Q 3
no ip route-cache
bridge-group 3
bridge-group 3 path-cost 400
!
interface BVI1
ip address 1.4.64.24 255.255.0.0
no ip route-cache
!
bridge 1 protocol ieee
bridge 1 route ip
bridge 1 priority 10000
bridge 2 protocol ieee
bridge 2 priority 12000
bridge 3 protocol ieee
bridge 3 priority 2900
!
line con 0
line vty 5 15
!
end

```

Displaying Spanning-Tree Status

To display the spanning-tree status, use one or more of the privileged EXEC commands in [Table 8-3](#):

Table 8-3 *Commands for Displaying Spanning-Tree Status*

Command	Purpose
show spanning-tree	Displays information on your network’s spanning tree.
show spanning-tree blocked-ports	Displays a list of blocked ports on this bridge.
show spanning-tree bridge	Displays status and configuration of this bridge.

Table 8-3 **Commands for Displaying Spanning-Tree Status (continued)**

Command	Purpose
show spanning-tree active	Displays spanning-tree information on active interfaces only.
show spanning-tree root	Displays a detailed summary of information on the spanning-tree root.
show spanning-tree interface <i>interface-id</i>	Displays spanning-tree information for the specified interface.
show spanning-tree summary [totals]	Displays a summary of port states or displays the total lines of the STP state section.

For information about other keywords for the **show spanning-tree** privileged EXEC command, refer to the *Cisco Aironet IOS Command Reference for Cisco Aironet Access Points and Bridges* for this release.



Configuring Cipher Suites and WEP

This chapter describes how to configure the cipher suites required to use WPA and CCKM authenticated key management, Wired Equivalent Privacy (WEP), WEP features including AES, Message Integrity Check (MIC), Temporal Key Integrity Protocol (TKIP), and broadcast key rotation. This chapter contains these sections:

- [Understanding Cipher Suites and WEP, page 9-2](#)
- [Configuring Cipher Suites and WEP, page 9-3](#)

Understanding Cipher Suites and WEP

This section describes how WEP and cipher suites protect traffic on your wireless LAN.

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/bridge can receive the access point/bridge's radio transmissions. Because WEP 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/bridge and client devices to keep the communication private. Both the access point/bridge 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, also called 802.1x 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. See [Chapter 10, “Configuring Authentication Types,”](#) for detailed information on EAP and other authentication types.

Cipher suites are sets of encryption and integrity algorithms designed to protect radio communication on your wireless LAN. You must use a cipher suite to enable Wi-Fi Protected Access (WPA) or Cisco Centralized Key Management (CCKM). Because cipher suites provide the protection of WEP while also allowing use of authenticated key management, Cisco recommends that you enable WEP by using the **encryption mode cipher** command in the CLI or by using the cipher drop-down menu in the web-browser interface. Cipher suites that contain TKIP provide the best security for your wireless LAN, and cipher suites that contain only WEP are the least secure.

These security features protect the data traffic on your wireless LAN:

- **AES-CCMP**—Based on the Advanced Encryption Standard (AES) defined in the National Institute of Standards and Technology's *FIPS Publication 197*, AES-CCMP is a symmetric block cipher that can encrypt and decrypt data using keys of 128, 192, and 256 bits. AES-CCMP is superior to WEP encryption and is defined in the IEEE 802.11i standard.



Note You can enable AES-CCMP only for 802.11g radios.

- **WEP (Wired Equivalent Privacy)**—WEP is an 802.11 standard encryption algorithm originally designed to provide your wireless LAN with the same level of privacy available on a wired LAN. However, the basic WEP construction is flawed, and an attacker can compromise the privacy with reasonable effort.
- **TKIP (Temporal Key Integrity Protocol)**—TKIP is a suite of algorithms surrounding WEP that is designed to achieve the best possible security on legacy hardware built to run WEP. TKIP adds four enhancements to WEP:
 - A per-packet key mixing function to defeat weak-key attacks
 - A new IV sequencing discipline to detect replay attacks
 - A cryptographic message integrity check (MIC), called *Michael*, to detect forgeries such as bit flipping and altering packet source and destination
 - An extension of IV space, to virtually eliminate the need for re-keying

- CKIP (Cisco Key Integrity Protocol)—Cisco's WEP key permutation technique based on an early algorithm presented by the IEEE 802.11i security task group.
- CMIC (Cisco Message Integrity Check)—Like TKIP's *Michael*, Cisco's message integrity check mechanism is designed to detect forgery attacks.
- Broadcast key rotation (also known as Group Key Update)—Broadcast key rotation allows the access point/bridge to generate the best possible random group key and update all key-management capable clients periodically. Wi-Fi Protected Access (WPA) also provides additional options for group key updates. See the [“Using WPA Key Management” section on page 10-7](#) for details on WPA.

**Note**

Client devices using static WEP cannot use the access point/bridge when you enable broadcast key rotation. When you enable broadcast key rotation, only wireless client devices using 802.1x authentication (such as LEAP, EAP-TLS, or PEAP) can use the access point/bridge.

Configuring Cipher Suites and WEP

These sections describe how to configure cipher suites, WEP and additional WEP features such as MIC, TKIP, and broadcast key rotation:

- [Creating WEP Keys, page 9-3](#)
- [Enabling Cipher Suites and WEP, page 9-6](#)
- [Enabling and Disabling Broadcast Key Rotation, page 9-7](#)

**Note**

WEP, TKIP, MIC, and broadcast key rotation are disabled by default.

Creating WEP Keys

**Note**

You need to configure static WEP keys only if your access point/bridge needs to support client devices that use static WEP. If all the client devices that associate to the access point/bridge use key management (WPA, CCKM, or 802.1x authentication) you do not need to configure static WEP keys.

Beginning in privileged EXEC mode, follow these steps to create a WEP key and set the key properties:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.

	Command	Purpose
Step 3	encryption [vlan <i>vlan-id</i>] key <i>1-4</i> size { 40 128 } <i>encryption-key</i> [0 7] [transmit-key]	Create a WEP key and set up its properties. • (Optional) Select the VLAN for which you want to create a key. • Name the key slot in which this WEP key resides. Up to 16 VLANs can be assigned. You can assign up to 4 WEP keys for each VLAN4 WEP keys to one of the VLANs. • Enter the key and set the size of the key, either 40-bit or 128-bit. 40-bit keys contain 10 hexadecimal digits; 128-bit keys contain 26 hexadecimal digits. • (Optional) Specify whether the key is encrypted (7) or unencrypted (0). • (Optional) Set this key as the transmit key. The key in slot 1 is the transmit key by default. Note If you configure static WEP with MIC or CMIC, the access point/bridge and associated client devices must use the same WEP key as the transmit key, and the key must be in the same key slot on the access point/bridge and the clients. Note Using security features such as authenticated key management can limit WEP key configurations. See the “WEP Key Restrictions” section on page 9-4 for a list of features that impact WEP keys.
Step 4	end	Return to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to create a 128-bit WEP key in slot 3 for VLAN 22 and sets the key as the transmit key:

```
ap# configure terminal
ap(config)# interface dot11radio 0
ap(config-if)# encryption vlan 22 key 3 size 128 12345678901234567890123456 transmit-key
ap(config-ssid)# end
```

WEP Key Restrictions

[Table 9-1](#) lists WEP key restrictions based on your security configuration.

Table 9-1 WEP Key Restrictions

Security Configuration	WEP Key Restriction
CCKM or WPA authenticated key management	Cannot configure a WEP key in key slot 1
LEAP or EAP authentication	Cannot configure a WEP key in key slot 4
Cipher suite with 40-bit WEP	Cannot configure a 128-bit key
Cipher suite with 128-bit WEP	Cannot configure a 40-bit key

Table 9-1 WEP Key Restrictions (continued)

Security Configuration	WEP Key Restriction
Cipher suite with TKIP	Cannot configure any WEP keys
Cipher suite with TKIP and 40-bit WEP or 128-bit WEP	Cannot configure a WEP key in key slot 1 and 4
Static WEP with MIC or CMIC	Access point and client devices must use the same WEP key as the transmit key, and the key must be in the same key slot on both access point/bridge and clients
Broadcast key rotation	Keys in slots 2 and 3 are overwritten by rotating broadcast keys Note Client devices using static WEP cannot use the access point/bridge when you enable broadcast key rotation. When you enable broadcast key rotation, only wireless client devices using 802.1x authentication (such as LEAP, EAP-TLS, or PEAP) can use the access point/bridge.

Example WEP Key Setup

Table 9-2 shows an example WEP key setup that would work for the access point/bridge and an associated device:

Table 9-2 WEP Key Setup Example

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

Because the access point/bridge's WEP key 1 is selected as the transmit key, WEP key 1 on the other device must have 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/bridge does not need to be set at all.


Note

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

Enabling Cipher Suites and WEP

Beginning in privileged EXEC mode, follow these steps to enable a cipher suite:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.
Step 3	encryption [vlan <i>vlan-id</i>] mode ciphers {[aes-ccm ckip cmic ckip-cmic tkip]} {[wep128 wep40]}	Enable a cipher suite containing the WEP protection you need. Table 9-3 lists guidelines for selecting a cipher suite that matches the type of authenticated key management you configure. (Optional) Select the VLAN for which you want to enable WEP and WEP features. - Set the cipher options and WEP level. You can combine TKIP with 128-bit or 40-bit WEP. Note If you enable a cipher suite with two elements (such as TKIP and 128-bit WEP), the second cipher becomes the group cipher. Note If you configure ckip, cmic, or ckip-cmic, you must also enable Aironet extensions. The command to enable Aironet extensions is dot11 extension aironet. Note You can also use the encryption mode wep command to set up static WEP. However, you should use encryption mode wep only if no clients that associate to the access point/bridge are capable of key management. See the <i>Cisco IOS Command Reference for Cisco Access Points and Bridges</i> for a detailed description of the encryption mode wep command. Note When you configure the cipher TKIP (not TKIP + WEP 128 or TKIP + WEP 40) for an SSID, the SSID must use WPA or CCKM key management. Client authentication fails on an SSID that uses the cipher TKIP without enabling WPA or CCKM key management.
Step 4	end	Return to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Use the **no** form of the encryption command to disable a cipher suite.

This example sets up a cipher suite for VLAN 22 that enables CKIP (unsupported), CMIC (unsupported), and 128-bit WEP.

```
ap# configure terminal
ap(config)# interface dot11radio 0
ap(config-if)# encryption vlan 22 mode ciphers ckip-cmic wep128
ap(config-if)# exit
```

Matching Cipher Suites with WPA and CCKM

If you configure your access point/bridge to use WPA or CCKM authenticated key management, you must select a cipher suite compatible with the authenticated key management type. [Table 9-3](#) lists the cipher suites that are compatible with WPA and CCKM.

Table 9-3 Cipher Suites Compatible with WPA and CCKM

Authenticated Key Management Types	Compatible Cipher Suites
CCKM	• encryption mode ciphers wep128 • encryption mode ciphers wep40 • encryption mode ciphers ckip • encryption mode ciphers cmic • encryption mode ciphers ckip-cmic • encryption mode ciphers tkip
WPA	• encryption mode ciphers tkip • encryption mode ciphers tkip wep128 • encryption mode ciphers tkip wep40



Note

When you configure the cipher TKIP (not **TKIP + WEP 128** or **TKIP + WEP 40**) for an SSID, the SSID must use WPA or CCKM key management. Client authentication fails on an SSID that uses the cipher TKIP without enabling WPA or CCKM key management.

For a complete description of WPA and CCKM and instructions for configuring authenticated key management, see the [“Using CCKM for Authenticated Clients”](#) section on page 10-6 and the [“Using WPA Key Management”](#) section on page 10-7.

Enabling and Disabling Broadcast Key Rotation

Broadcast key rotation is disabled by default.



Note

Client devices using static WEP cannot use the access point/bridge when you enable broadcast key rotation. When you enable broadcast key rotation, only wireless client devices using 802.1x authentication (such as LEAP, EAP-TLS, or PEAP) can use the access point/bridge.

Beginning in privileged EXEC mode, follow these steps to enable broadcast key rotation:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.

	Command	Purpose
Step 3	broadcast-key change <i>seconds</i> [vlan <i>vlan-id</i>] [membership-termination] [capability-change]	Enable broadcast key rotation. • Enter the number of seconds between each rotation of the broadcast key. • (Optional) Enter a VLAN for which you want to enable broadcast key rotation. • (Optional) If you enable WPA authenticated key management, you can enable additional circumstances under which the access point/bridge changes and distributes the WPA group key. – Membership termination—the access point/bridge generates and distributes a new group key when any authenticated client device disassociates from the access point/bridge. This feature protects the privacy of the group key for associated clients. However, it might generate some overhead if clients on your network roam frequently. – Capability change—the access point/bridge generates and distributes a dynamic group key when the last non-key management (static WEP) client disassociates, and it distributes the statically configured WEP key when the first non-key management (static WEP) client authenticates. In WPA migration mode, this feature significantly improves the security of key-management capable clients when there are no static-WEP clients associated to the access point/bridge. See Chapter 10, “Configuring Authentication Types,” for detailed instructions on enabling authenticated key management.
Step 4	end	Return to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Use the **no** form of the encryption command to disable broadcast key rotation.

This example enables broadcast key rotation on VLAN 22 and sets the rotation interval to 300 seconds:

```

apap# configure terminal
ap(config)# interface dot11radio 0
ap(config-if)# broadcast-key vlan 22 change 300
ap(config-ssid)# end

```



Configuring Authentication Types

This chapter describes how to configure authentication types on the access point/bridge. This chapter contains these sections:

- [Understanding Authentication Types, page 10-2](#)
- [Configuring Authentication Types, page 10-9](#)
- [Matching Authentication Types on Root and Non-Root Access Point/Bridges, page 10-15](#)

Understanding Authentication Types

This section describes the authentication types that you can configure on the access point/bridge. The authentication types are tied to the SSIDs that you configure for the access point. If you want to serve different types of client devices with the same access point, you can configure multiple SSIDs. See [Chapter 7, “Configuring Multiple SSIDs,”](#) for complete instructions on configuring multiple SSIDs.

Before a wireless client device can communicate on your network through the access point/bridge, it must authenticate to the access point using open or shared-key authentication. For maximum security, client devices should also authenticate to your network using MAC-address or EAP authentication, authentication types that rely on an authentication server on your network.

**Note**

By default, the access point/bridge sends reauthentication requests to the authentication server with the service-type attribute set to authenticate-only. However, some Microsoft IAS servers do not support the authenticate-only service-type attribute. Changing the service-type attribute to login-only ensures that Microsoft IAS servers recognize reauthentication requests from the access point. Use the **dot11 aaa authentication attributes service-type login-only** global configuration command to set the service-type attribute in reauthentication requests to login-only.

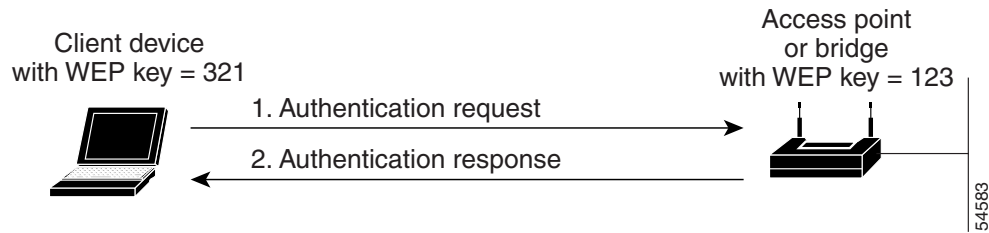
The access point/bridge uses several authentication mechanisms or types and can use more than one at the same time. These sections explain each authentication type:

- [Open Authentication to the Access Point/Bridge, page 10-2](#)
- [Shared Key Authentication to the Access Point/Bridge, page 10-3](#)
- [EAP Authentication to the Network, page 10-4](#)
- [MAC Address Authentication to the Network, page 10-5](#)
- [Combining MAC-Based, EAP, and Open Authentication, page 10-6](#)
- [Using CCKM for Authenticated Clients, page 10-6](#)
- [Using WPA Key Management, page 10-7](#)
- [Software and Firmware Requirements for WPA and WPA-TKIP, page 10-9](#)
- [Assigning Authentication Types to an SSID, page 10-10](#)
- [Assigning Authentication Types to an SSID, page 10-10](#)
- [Configuring Authentication Holdoffs, Timeouts, and Intervals, page 10-14](#)

Open Authentication to the Access Point/Bridge

Open authentication allows any 1300 series access point/bridge to authenticate and then attempt to communicate with another 1300 series access point/bridge. Using open authentication, a non-root access point/bridge can authenticate to a root access point/bridge, but the non-root access point/bridge can communicate only if its WEP keys match the root access point/bridge's. An access point/bridge that is not using WEP does not attempt to authenticate with an access point/bridge that is using WEP. Open authentication does not rely on a RADIUS server on your network.

[Figure 10-1](#) shows the authentication sequence between a non-root access point/bridge trying to authenticate and a root access point/bridge using open authentication. In this example, the device's WEP key does not match the access point/bridge's key, so it can authenticate but not pass data. The same scenario occurs when a client attempts to associate to the access point/bridge configured as an a root access point or repeater access points with clients.

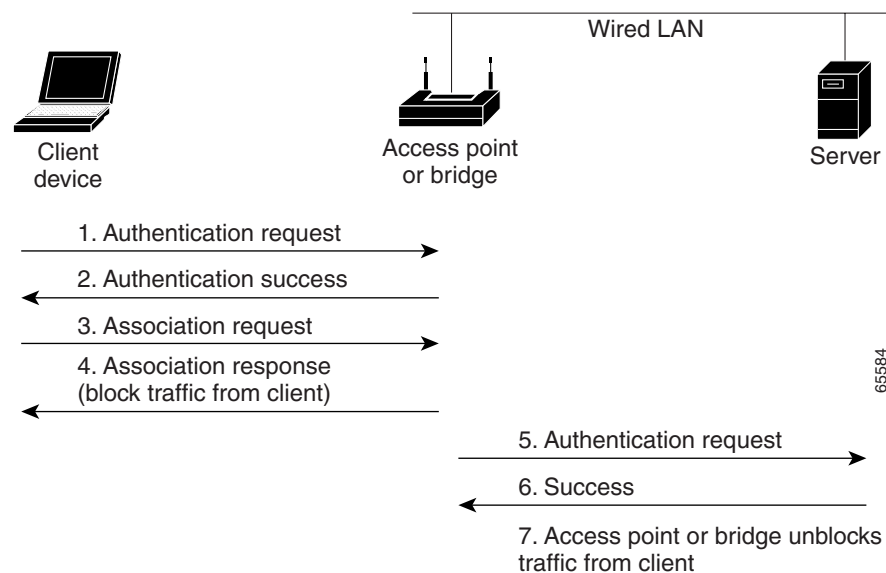
Figure 10-1 Sequence for Open Authentication

Shared Key Authentication to the Access Point/Bridge

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 root access point/bridge sends an unencrypted challenge text string to other access point/bridges attempting to communicate with the root access point/bridge. The access point/bridge requesting authentication encrypts the challenge text and sends it back to the root access point/bridge. If the challenge text is encrypted correctly, the root access point/bridge allows the requesting device to authenticate. Both the unencrypted challenge and the encrypted challenge can be monitored, however, which leaves the root access point/bridge 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 10-2 shows the authentication sequence between a device trying to authenticate and an access point/bridge using shared key authentication. In this example the device's WEP key matches the access point/bridge's key, so it can authenticate and communicate. The same sequence occurs when the bridge is configured as a root access point or repeater access point with clients.

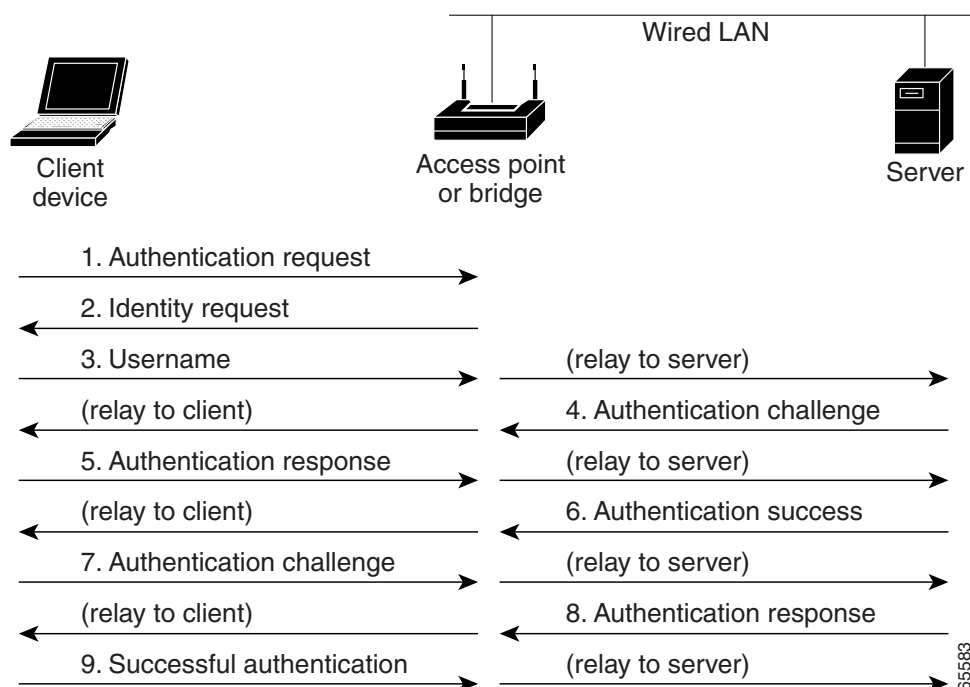
Figure 10-2 Sequence for Shared Key Authentication

EAP Authentication to the Network

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 root access point/bridge helps another access point/bridge and the RADIUS server to perform mutual authentication and derive a dynamic unicast WEP key. The RADIUS server sends the WEP key to the root access point/bridge, which uses it for all unicast data signals that it sends to or receives from the non-root access point/bridge. The root access point/bridge also encrypts its broadcast WEP key (entered in the access point/bridge's WEP key slot 1) with the non-root access point/bridge's unicast key and sends it to the non-root access point/bridge.

When you enable EAP on your access point/bridges, authentication to the network occurs in the sequence shown in [Figure 10-3](#):

Figure 10-3 Bridge Sequence for EAP Authentication



In Steps 1 through 9 in [Figure 10-3](#), a non-root access point/bridge or wireless client device and a RADIUS server on the wired LAN use 802.1x and EAP to perform a mutual authentication through the root access point/bridge. The RADIUS server sends an authentication challenge to the non-root access point/bridge or client. The non-root access point/bridge 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 non-root access point/bridge or client. When the RADIUS server authenticates the non-root access point/bridge, the process repeats in reverse, and the non-root access point/bridge or client authenticates the RADIUS server.

When mutual authentication is complete, the RADIUS server and the non-root access point/bridge determine a WEP key that is unique to the non-root access point/bridge and provides the non-root access point/bridge with the appropriate level of network access, thereby approximating the level of security in a wired switched segment to an individual desktop. The non-root access point/bridge 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 root access point/bridge. The root access point/bridge encrypts its broadcast key with the session key and sends the encrypted broadcast key to the non-root access point/bridge, which uses the session key to decrypt it. The non-root access point/bridge and the root access point/bridge 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/bridge 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 [“Assigning Authentication Types to an SSID” section on page 10-10](#) for instructions on setting up EAP on the access point/bridge.

**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/bridge and to your network.

MAC Address Authentication to the Network

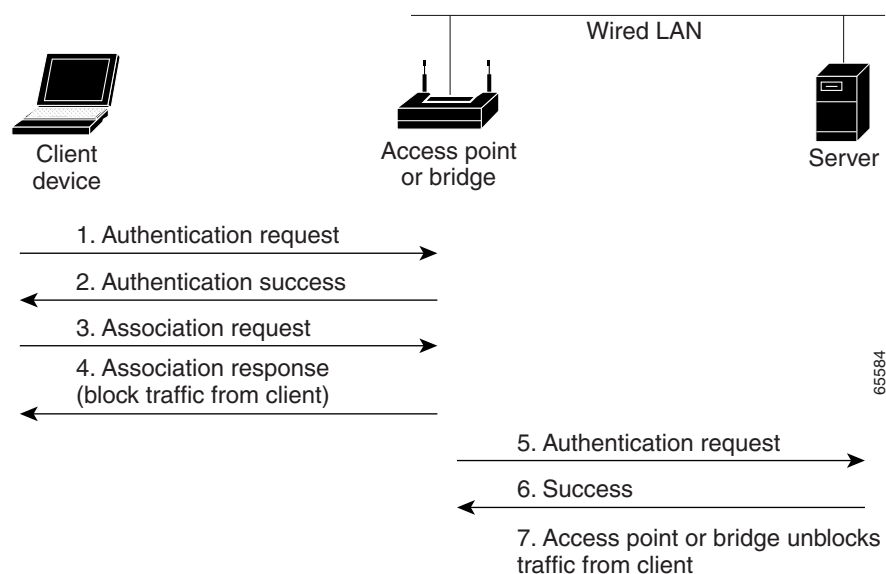
The access point/bridge relays the wireless client device's MAC address to a RADIUS server on your network, and the server checks the address against a list of allowed MAC addresses. Intruders can create counterfeit MAC addresses, so MAC-based authentication is less secure than EAP authentication. However, MAC-based authentication provides an alternate authentication method for client devices that do not have EAP capability. See the [“Assigning Authentication Types to an SSID” section on page 10-10](#) for instructions on enabling MAC-based authentication.

**Tip**

If you don't have a RADIUS server on your network, you can create a list of allowed MAC addresses on the access point/bridge's Advanced Security: MAC Address Authentication page. Devices with MAC addresses not on the list are not allowed to authenticate.

Figure 10-4 shows the authentication sequence for MAC-based authentication.

Figure 10-4 Sequence for MAC-Based 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 [“Assigning Authentication Types to an SSID”](#) section on page 10-10 for instructions on setting up this combination of authentications.

Using CCKM for Authenticated Clients

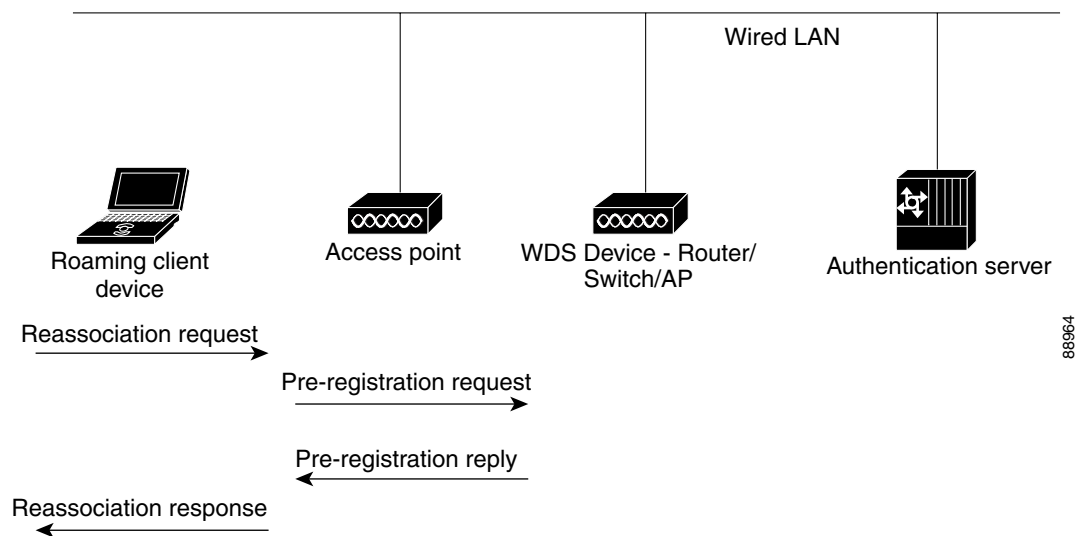
Using Cisco Centralized Key Management (CCKM), authenticated client devices can roam from one access point to another without any perceptible delay during reassociation. An access point on your network provides Wireless Domain Services (WDS) and creates a cache of security credentials for CCKM-enabled client devices on the subnet. The WDS access point’s cache of credentials dramatically reduces the time required for reassociation when a CCKM-enabled client device roams to a new access point. When a client device roams, the WDS access point forwards the client’s security credentials to the new access point, and the reassociation process is reduced to a two-packet exchange between the roaming client and the new access point. Roaming clients reassociate so quickly that there is no perceptible delay in voice or other time-sensitive applications. See the [“Assigning Authentication Types to an SSID”](#) section on page 10-10 for instructions on enabling CCKM on your access point. See the [“Configuring Access Point/Bridges as Potential WDS Devices”](#) section on page 11-8 for detailed instructions on setting up a WDS access point on your wireless LAN.

**Note**

The RADIUS-assigned VLAN feature is not supported for client devices that associate using SSIDs with CCKM enabled.

Figure 10-5 shows the reassociation process using CCKM.

Figure 10-5 Client Reassociation Using CCKM



Using WPA Key Management

Wi-Fi Protected Access (WPA) is a standards-based, interoperable security enhancement that strongly increases the level of data protection and access control for existing and future wireless LAN systems. It is derived from and will be forward-compatible with the upcoming IEEE 802.11i standard. WPA leverages TKIP (Temporal Key Integrity Protocol) for data protection and 802.1X for authenticated key management.

WPA key management supports two mutually exclusive management types: WPA and WPA-Pre-shared key (WPA-PSK). Using WPA key management, non-root access point/bridges and the authentication server authenticate to each other using an EAP authentication method, and the non-root access point/bridge and server generate a pairwise master key (PMK). Using WPA, the server generates the PMK dynamically and passes it to the root access point/bridge. Using WPA-PSK, however, you configure a pre-shared key on both the non-root access point/bridge and the root access point/bridge, and that pre-shared key is used as the PMK.

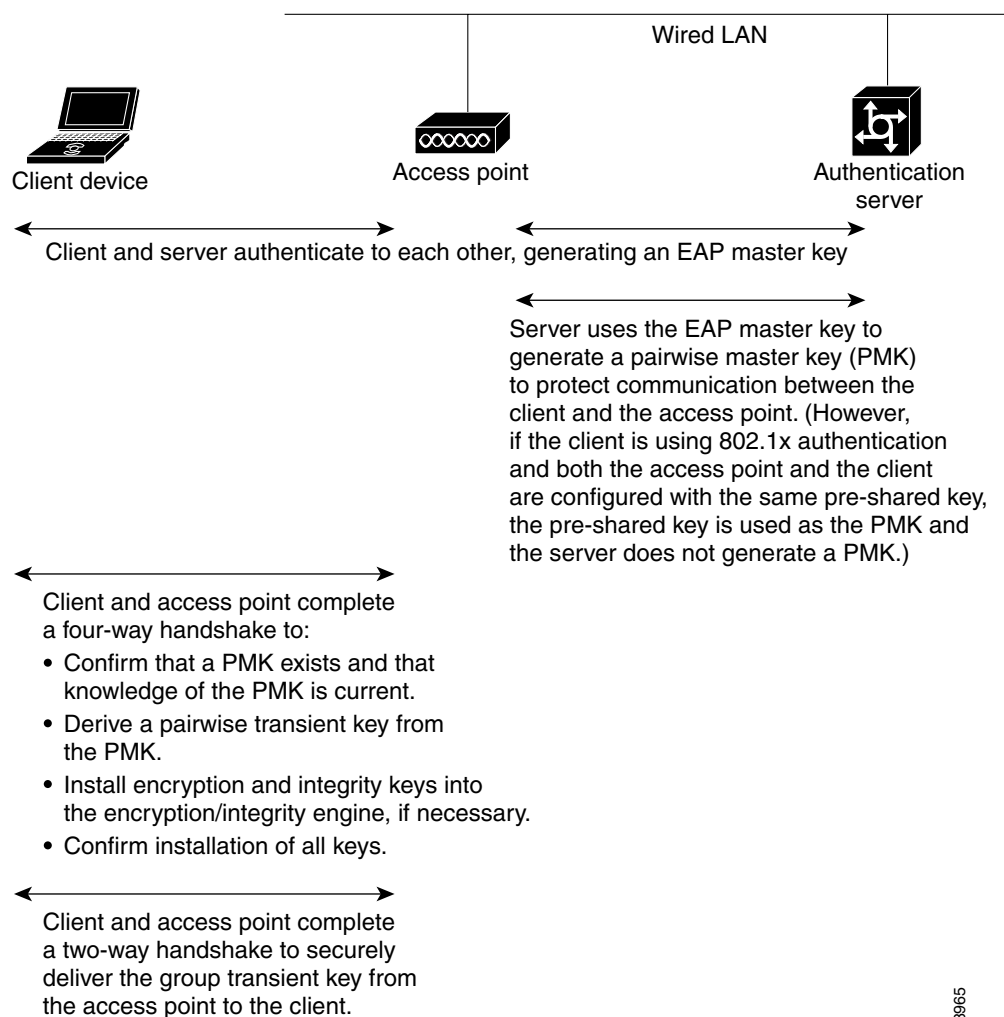
**Note**

Unicast and multicast cipher suites advertised in the WPA information element (and negotiated during 802.11 association) may potentially mismatch with the cipher suite supported in an explicitly assigned VLAN. If the RADIUS server assigns a new VLAN ID which uses a different cipher suite from the previously negotiated cipher suite, there is no way for the root access point/bridge and the non-root access point/bridge to switch back to the new cipher suite. Currently, the WPA and CCKM protocols do not allow the cipher suite to be changed after the initial 802.11 cipher negotiation phase. In this scenario, the non-root access point/bridge is disassociated from the wireless LAN.

See the “[Assigning Authentication Types to an SSID](#)” section on page 10-10 for instructions on configuring WPA key management on your access point/bridge.

Figure 10-6 shows the WPA key management process.

Figure 10-6 WPA Key Management Process



Software and Firmware Requirements for WPA and WPA-TKIP

Table 10-1 lists the firmware and software requirements required on access points and Cisco Aironet client devices to support WPA key management and WPA-TKIP encryption protocols.

To support the security combinations in Table 10-1, your Cisco Aironet access points and Cisco Aironet client devices must run the following software and firmware versions:

- Cisco IOS Release 12.2(13)JA or later on access points
- Install Wizard version 1.2 for 340, 350, and CB20A client devices, which includes these components:
 - PC, LM, and PCI card driver version 8.4
 - Mini PCI and PC-cardbus card driver version 3.7
 - Aironet Client Utility (ACU) version 6.2
 - Client firmware version 5.30.13

Table 10-1 Software and Firmware Requirements for WPA, CCKM, CKIP, and WPA-TKIP

Key Management and Encryption Protocol	Third Party Host Supplicant ¹ Required?	Supported Platform Operating Systems
LEAP with WPA-TKIP	No	Windows XP and 2000
LEAP with WPA	No	Windows XP and 2000
Host-based EAP (such as PEAP and EAP-TLS) with WPA	No ²	Windows XP
Host-based EAP (such as PEAP and EAP-TLS) with WPA	Yes	Windows 2000
WPA-PSK Mode	No ²	Windows XP
WPA-PSK Mode	Yes	Windows 2000

1. Such as Funk Odyssey Client supplicant version 2.2 or Meetinghouse Data Communications Aegis Client version 2.1.
2. Windows XP does not require a third-party supplicant, but you must install Windows XP Service Pack 1 and Microsoft support patch 815485.



Note

When you configure **TKIP**-only cipher encryption (not **TKIP + WEP 128** or **TKIP + WEP 40**) on any radio interface or VLAN, every SSID on that radio or VLAN must be set to use WPA key management. If you configure TKIP on a radio or VLAN but you do not configure key management on the SSIDs, client authentication fails on the SSIDs.

Configuring Authentication Types

This section describes how to configure authentication types. You attach configuration types to the access point/bridge's SSID. See Chapter 7, "Configuring Multiple SSIDs," for details on setting up the access point/bridge SSID. This section contains these topics:

- [Assigning Authentication Types to an SSID, page 10-10](#)
- [Configuring Authentication Holdoffs, Timeouts, and Intervals, page 10-14](#)

Assigning Authentication Types to an SSID

Beginning in privileged EXEC mode, follow these steps to configure authentication types for SSIDs:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.
Step 3	ssid <i>ssid-string</i>	Create an SSID and enter SSID configuration mode for the new SSID. The SSID can consist of up to 32 alphanumeric characters. SSIDs are case sensitive. Note Do not include spaces in SSIDs.
Step 4	authentication open [<i>mac-address list-name</i> [alternate]] [<i>eap list-name</i>]	(Optional) Set the authentication type to open for this SSID. Open authentication allows any device to authenticate and then attempt to communicate with the access point/bridge. (Optional) Set the SSID's authentication type to open with EAP authentication. The access point/bridge forces all other client devices to perform EAP authentication before they are allowed to join the network. For <i>list-name</i>, specify the authentication method list. Click this link for more information on method lists: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fsaaa/scfathen.htm#xtocid2 Use the alternate keyword to allow client devices to join the network using either MAC or EAP authentication; clients that successfully complete either authentication are allowed to join the network. (Optional) Set the SSID's authentication type to open with EAP authentication. The access point forces all client devices to perform EAP authentication before they are allowed to join the network. For <i>list-name</i>, specify the authentication method list. Note A access point/bridge configured for EAP authentication forces all access point/bridges that associate to perform EAP authentication. Client devices that do not use EAP cannot communicate with the access point/bridge.
Step 5	authentication shared [<i>mac-address list name</i>] [<i>eap list-name</i>]	(Optional) Set the authentication type for the SSID to shared key. Note Because of shared key's security flaws, Cisco recommends that you avoid using it. Note You can assign shared key authentication to only one SSID. (Optional) Set the SSID's authentication type to shared key with EAP authentication. For <i>list-name</i>, specify the authentication method list.

	Command	Purpose
Step 6	authentication network-eap <i>list-name</i> [<i>mac-address list name</i>]	(Optional) Set the authentication type for the SSID to Network-EAP. 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. However, the access point does not force all client devices to perform EAP authentication. (Optional) Set the SSID's authentication type to Network-EAP with MAC address authentication. All client devices that associate to the access point are required to perform MAC-address authentication. For <i>list-name</i> , specify the authentication method list.
Step 7	authentication key-management { [wpa] } [optional]	(Optional) Set the authentication type for the SSID to WPA. If you use the optional keyword, client devices other than WPA clients can use this SSID. If you do not use the optional keyword, only WPA client devices are allowed to use the SSID. To enable WPA for an SSID, you must also enable Open authentication or Network-EAP or both. Note Before you can enable WPA, you must set the encryption mode for the SSID's VLAN to one of the cipher suite options. See the “Configuring Cipher Suites and WEP” section on page 9-3 for instructions on configuring the VLAN encryption mode. Note If you enable WPA for an SSID without a pre-shared key, the key management type is WPA. If you enable WPA with a pre-shared key, the key management type is WPA-PSK. See the “Configuring Additional WPA Settings” section on page 10-13 for instructions on configuring a pre-shared key.
Step 8	end	Return to privileged EXEC mode.
Step 9	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Use the **no** form of the SSID commands to disable the SSID or to disable SSID features.

This example sets the authentication type for the SSID access point/bridgeman to open with EAP authentication. Access points and bridges using the access point/bridge an SSID attempt EAP authentication using a server named *adam*.

```
ap# configure terminal
ap(config)# configure interface dot11radio 0
ap(config-if)# ssid bridgeman
ap(config-ssid)# authentication open eap adam
ap(config-ssid)# end
```

The configuration on non-root access point/bridges associated to this access point/bridge would also contain these commands:

```
ap(config)# configure interface dot11radio 0
ap(config-if)# ssid bridgeman
ap(config-ssid)# authentication client username bridge7 password catch22
ap(config-ssid)# authentication open eap adam
```

This example sets the authentication type for the SSID access point/bridget to network-EAP with a static WEP key. EAP-enabled access point/bridges using the access point/bridget SSID attempt EAP authentication using a server named *eve*, and access point/bridges using static WEP rely on the static WEP key.

```
ap# configure terminal
ap(config)# configure interface dot11radio 0
ap(config-if)# encryption key 2 size 128 12345678901234567890123456
ap(config-if)# ssid bridget
ap(config-ssid)# authentication network-eap eve
ap(config-ssid)# end
```

The configuration on non-root access point/bridges associated to this access point/bridge would also contain these commands:

```
ap(config)# configure interface dot11radio 0
ap(config-if)# ssid bridget
ap(config-ssid)# authentication client username bridge11 password 99bottles
```

Configuring WPA Migration Mode

WPA migration mode allows these client device types to associate to the access point/bridge using the same SSID:

- WPA clients capable of TKIP and authenticated key management
- 802.1X-2001 clients (such as legacy LEAP clients and clients using TLS) capable of authenticated key management but not TKIP
- Static-WEP clients not capable of TKIP or authenticated key management

If all three client types associate using the same SSID, the multicast cipher suite for the SSID must be WEP. If only the first two types of clients use the same SSID the multicast key can be dynamic, but if the static-WEP clients use the SSID, the key must be static. The access point/bridge can switch automatically between a static and a dynamic group key to accommodate associated client devices. To support all three types of clients on the same SSID, you must configure the static key in key slots 2 or 3.

To set up an SSID for WPA migration mode, configure these settings:

- WPA optional
- A cipher suite containing TKIP and 40-bit or 128-bit WEP
- A static WEP key in key slot 2 or 3

This example sets the SSID migrate for WPA migration mode:

```
ap# configure terminal
ap(config)# interface dot11radio 0
ap(config-if)# encryption mode cipher tkip wep128
ap(config-if)# encryption key 3 size 128 12345678901234567890123456 transmit-key
ap(config-if)# ssid migrate
ap(config-ssid)# authentication open
ap(config-ssid)# authentication network-eap adam
ap(config-ssid)# authentication key-management wpa optional
ap(config-ssid)# wpa-psk ascii batmobile65
ap(config-ssid)# exit
```


Configuring the Root Access Point/Bridge to Interact with the WDS Device

To support non-root access point/bridges using CCKM, your root access point/bridge must interact with the WDS device on your network, and your authentication server must be configured with a username and password for the root access point/bridge. For detailed instructions on configuring WDS and CCKM on your wireless LAN, see Chapter 11 in the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*.

On your root access point/bridge, enter this command in global configuration mode:

```
ap(config)# wlccp ap username username password password
```

You must configure the same username and password pair when you set up the root access point/bridge as a client on your authentication server.

Configuring Additional WPA Settings

Use two optional settings to configure a pre-shared key on the access point/bridge and adjust the frequency of group key updates.

Setting a Pre-Shared Key

To support WPA on a wireless LAN where 802.1x-based authentication is not available, you must configure a pre-shared key on the access point/bridge. You can enter the pre-shared key as ASCII or hexadecimal characters. If you enter the key as ASCII characters, you enter between 8 and 63 characters, and the access point/bridge expands the key using the process described in the *Password-based Cryptography Standard* (RFC2898). If you enter the key as hexadecimal characters, you must enter 64 hexadecimal characters.

Configuring Group Key Updates

In the last step in the WPA process, the access point/bridge distributes a group key to the authenticated client device. You can use these optional settings to configure the access point to change and distribute the group key based on client association and disassociation:

- Membership termination—the access point generates and distributes a new group key when any authenticated device disassociates from the access point/bridge. This feature keeps the group key private for associated devices, but it might generate some overhead traffic if clients on your network roam frequently among access points.
- Capability change—the access point/bridge generates and distributes a dynamic group key when the last non-key management (static WEP) client disassociates, and it distributes the statically configured WEP key when the first non-key management (static WEP) client authenticates. In WPA migration mode, this feature significantly improves the security of key-management capable clients when there are no static-WEP clients associated to the access point/bridge.

Beginning in privileged EXEC mode, follow these steps to configure a WPA pre-shared key and group key update options:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.
Step 3	ssid ssid-string	Enter SSID configuration mode for the SSID.

	Command	Purpose
Step 4	wpa-psk { hex ascii } [0 7] <i>encryption-key</i>	Enter a pre-shared key for access point/bridges using WPA that also use static WEP keys. Enter the key using either hexadecimal or ASCII characters. If you use hexadecimal, you must enter 64 hexadecimal characters to complete the 256-bit key. If you use ASCII, you must enter a minimum of 8 letters, numbers, or symbols, and the access point/bridge expands the key for you. You can enter a maximum of 63 ASCII characters.
Step 5	end	Return to privileged EXEC mode.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to configure a pre-shared key for non-root access point/bridges using WPA and static WEP, with group key update options:

```
ap# configure terminal
ap(config)# configure interface dot11radio 0
ap(config-if)# ssid batman
ap(config-ssid)# wpa-psk ascii batmobile65
ap(config-ssid)# end
```

Configuring Authentication Holdoffs, Timeouts, and Intervals

Beginning in privileged EXEC mode, follow these steps to configure holdoff times, reauthentication periods, and authentication timeouts for non-root access point/bridges and client devices authenticating through your root access point/bridge:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	dot11 holdoff-time <i>seconds</i>	Enter the number of seconds a root access point/bridge must wait before it disassociates and idle client. Enter a value from 1 to 65555 seconds.
Step 3	interface dot11radio 0	Enter interface configuration mode for the radio interface.
Step 4	dot1x client-timeout <i>seconds</i>	Enter the number of seconds the bridge should wait for a reply from a non-root access point/bridge attempting to authenticate before the authentication fails. Enter a value from 1 to 65555 seconds.

	Command	Purpose
Step 5	dot1x reauth-period <i>seconds</i> [<i>server</i>]	Enter the interval in seconds that the access point/bridge waits before forcing an authenticated non-root access point/bridge to reauthenticate. (Optional) Enter the server keyword to configure the access point/bridge to use the reauthentication period specified by the authentication server. If you use this option, configure your authentication server with RADIUS attribute 27, Session-Timeout. This attribute sets the maximum number of seconds of service to be provided to the non-root access point/bridge before termination of the session or prompt. The server sends this attribute to the root access point/bridge when a non-root access point/bridge performs EAP authentication.
Step 6	end	Return to privileged EXEC mode.
Step 7	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Use the **no** form of these commands to reset the values to default settings.

Matching Authentication Types on Root and Non-Root Access Point/Bridges

To use the authentication types described in this section, the access point/bridge authentication settings must match the authentication settings on the client adapters that associate to the access point. Refer to the *Cisco Aironet Wireless LAN Client Adapters Installation and Configuration Guide for Windows* for instructions on setting authentication types on wireless client adapters. Refer to [Chapter 9, “Configuring Cipher Suites and WEP,”](#) for instructions on configuring cipher suites and WEP on the access point.

[Table 10-2](#) lists the client and access point settings required for each authentication type.



Note

Some non-Cisco Aironet client adapters do not perform 802.1x authentication to the access point unless you configure **Open authentication with EAP**. To allow both Cisco Aironet clients using LEAP and non-Cisco Aironet clients using LEAP to associate using the same SSID, you might need to configure the SSID for both **Network EAP** authentication and **Open authentication with EAP**.

Table 10-2 Client and Access Point Security Settings

Security Feature	Client Setting	Access Point Setting
Static WEP with open authentication	Create a WEP key and enable Use Static WEP Keys and Open Authentication	Set up and enable WEP and enable Open Authentication for the SSID
Static WEP with shared key authentication	Create a WEP key and enable Use Static WEP Keys and Shared Key Authentication	Set up and enable WEP and enable Shared Key Authentication for the SSID

Table 10-2 Client and Access Point Security Settings (continued)

Security Feature	Client Setting	Access Point Setting
LEAP authentication	Enable LEAP	Set up and enable WEP and enable Network-EAP for the SSID ¹
802.1x authentication	Enable LEAP	Select a cipher suite and enable Network-EAP for the SSID
802.1x authentication and WPA	Enable any 802.1x authentication method	Select a cipher suite and enable Open authentication and WPA for the SSID (you can also enable Network-EAP authentication in addition to or instead of Open authentication) Note To allow both WPA clients and non-WPA clients to use the SSID, enable optional WPA.
802.1x authentication and WPA-PSK	Enable any 802.1x authentication method	Select a cipher suite and enable Open authentication and WPA for the SSID (you can also enable Network-EAP authentication in addition to or instead of Open authentication). Enter a WPA pre-shared key. Note To allow both WPA clients and non-WPA clients to use the SSID, enable optional WPA.
EAP-TLS authentication		
If using ACU to configure card	Enable Host Based EAP and Use Dynamic WEP Keys in ACU and select Enable network access control using IEEE 802.1X and Smart Card or Other Certificate as the EAP Type in Windows 2000 (with Service Pack 3) or Windows XP	Set up and enable WEP and enable EAP and Open authentication for the SSID
If using Windows XP to configure card	Select Enable network access control using IEEE 802.1X and Smart Card or other Certificate as the EAP Type	Set up and enable WEP and enable EAP and Open Authentication for the SSID

Table 10-2 Client and Access Point Security Settings (continued)

Security Feature	Client Setting	Access Point Setting
PEAP authentication		
If using ACU to configure card	Enable Host Based EAP and Use Dynamic WEP Keys in ACU and select Enable network access control using IEEE 802.1X and PEAP as the EAP Type in Windows 2000 (with Service Pack 3) or Windows XP	Set up and enable WEP and enable EAP and Open authentication for the SSID
If using Windows XP to configure card	Select Enable network access control using IEEE 802.1X and PEAP as the EAP Type	Set up and enable WEP and enable Require EAP and Open Authentication for the SSID

1. Some non-Cisco Aironet client adapters do not perform 802.1x authentication to the access point unless you configure **Open authentication with EAP**. To allow both Cisco Aironet clients using LEAP and non-Cisco Aironet clients using LEAP to associate using the same SSID, you might need to configure the SSID for both **Network EAP** authentication and **Open authentication with EAP**.



Configuring WDS, Fast Secure Roaming, Radio Management, and Wireless Intrusion Detection Services

This chapter describes how to configure your access point/bridges for wireless domain services (WDS), fast, secure roaming of client devices, radio management, and wireless intrusion detection services (WIDS). This chapter contains these sections:

- [Understanding WDS, page 11-2](#)
- [Understanding Fast Secure Roaming, page 11-3](#)
- [Understanding Radio Management, page 11-4](#)
- [Understanding Layer 3 Mobility, page 11-4](#)
- [Understanding Wireless Intrusion Detection Services, page 11-6](#)
- [Configuring WDS, page 11-6](#)
- [Configuring Fast Secure Roaming, page 11-21](#)
- [Configuring Radio Management, page 11-25](#)
- [Configuring Access Points to Participate in WIDS, page 11-27](#)

For instructions on configuring WDS on a switch's Wireless LAN Services Module (WLSM), refer to the *Catalyst 6500 Series Wireless LAN Services Module Installation and Configuration Note*.

Understanding WDS

When you configure Wireless Domain Services on your network, access point/bridges on your wireless LAN use the WDS device (either an access point/bridge, an Integrated Services Router, or a switch configured as the WDS device) to provide fast, secure roaming for client devices and to participate in radio management. If you use a switch as the WDS device, the switch must be equipped with a Wireless LAN Services Module (WLSM). An access point/bridge configured as the WDS device supports up to 60 participating access points, an Integrated Services Router (ISR) configured as the WDS device supports up to 100 participating access points, and a WLSM-equipped switch supports up to 300 participating access points.

Fast, secure roaming provides rapid reauthentication when a client device roams from one access point to another, preventing delays in voice and other time-sensitive applications.

Access points participating in radio management forward information about the radio environment (such as possible rogue access points and client associations and disassociations) to the WDS device. The WDS device aggregates the information and forwards it to a wireless LAN solution engine (WLSE) device on your network.

Role of the WDS Device

The WDS device performs several tasks on your wireless LAN:

- Advertises its WDS capability and participates in electing the best WDS device for your wireless LAN. When you configure your wireless LAN for WDS, you set up one device as the main WDS candidate and one or more additional devices as backup WDS candidates. If the main WDS device goes off line, one of the backup WDS devices takes its place.
- Authenticates all access points in the subnet and establishes a secure communication channel with each of them.
- Collects radio data from access points in the subnet, aggregates the data, and forwards it to the WLSE device on your network.
- Acts as a pass-through for all 802.1x-authenticated client devices associated to participating access points.
- Registers all client devices in the subnet that use dynamic keying, establishes session keys for them, and caches their security credentials. When a client roams to another access point, the WDS device forwards the client's security credentials to the new access point.

[Table 11-1](#) lists the number of participating access points supported by the platforms that can be configured as a WDS device: an access point, an ISR, or a WLSM-equipped switch.

Table 11-1 *Participating Access Points Supported by WDS Devices*

Unit Configured as WDS Device	Participating Access Points Supported
Access point that also serves client devices	30
Access point with radio interfaces disabled	60
Integrated Services Router (ISR)	100 (depending on ISR platform)
WLSM-equipped switch	300

Role of Access Points Using the WDS Device

The access points on your wireless LAN interact with the WDS device in these activities:

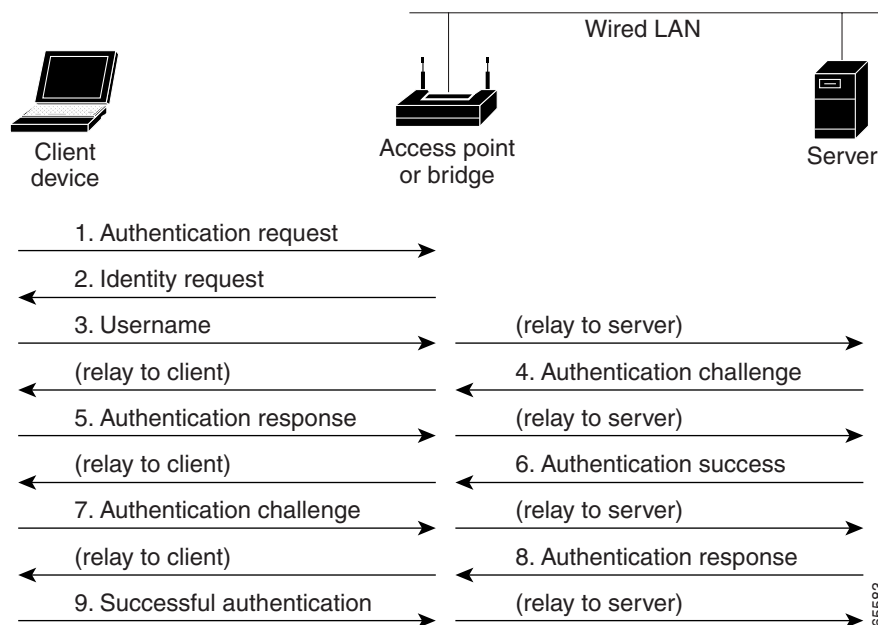
- Discover and track the current WDS device and relay WDS advertisements to the wireless LAN.
- Authenticate with the WDS device and establish a secure communication channel to the WDS device.
- Register associated client devices with the WDS device.
- Report radio data to the WDS device.

Understanding Fast Secure Roaming

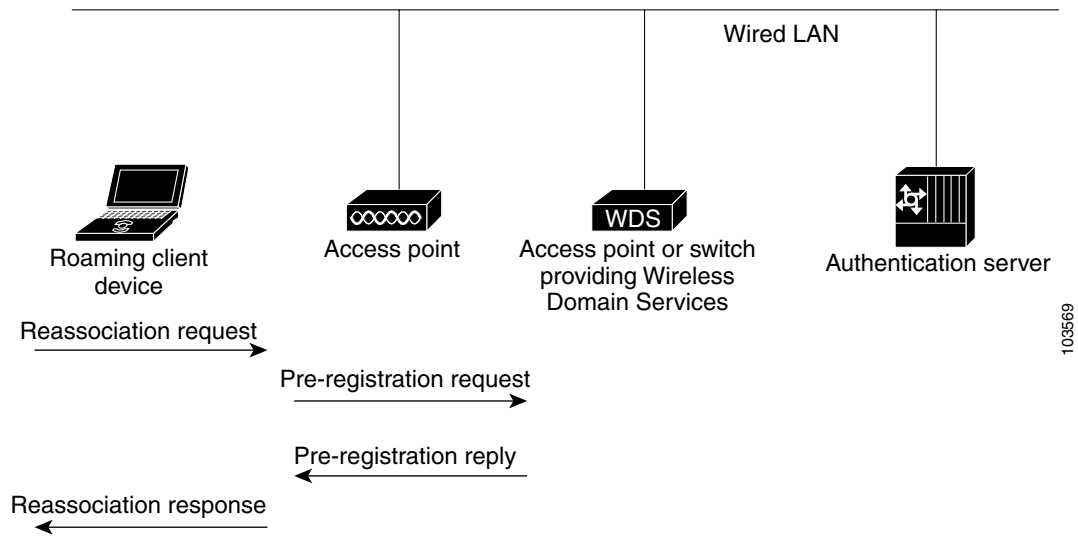
Access points in many wireless LANs serve mobile client devices that roam from access point to access point throughout the installation. Some applications running on client devices require fast reassociation when they roam to a different access point. Voice applications, for example, require seamless roaming to prevent delays and gaps in conversation.

During normal operation, LEAP-enabled client devices mutually authenticate with a new access point by performing a complete LEAP authentication, including communication with the main RADIUS server, as in [Figure 11-1](#).

Figure 11-1 Client Authentication Using a RADIUS Server



When you configure your wireless LAN for fast, secure roaming, however, LEAP-enabled client devices roam from one access point to another without involving the main RADIUS server. Using Cisco Centralized Key Management (CCKM), a device configured to provide Wireless Domain Services (WDS) takes the place of the RADIUS server and authenticates the client so quickly that there is no perceptible delay in voice or other time-sensitive applications. [Figure 11-2](#) shows client authentication using CCKM.

Figure 11-2 Client Reassociation Using CCKM and a WDS Access Point

The WDS device maintains a cache of credentials for CCKM-capable client devices on your wireless LAN. When a CCKM-capable client roams from one access point to another, the client sends a reassociation request to the new access point, and the new access point relays the request to the WDS device. The WDS device forwards the client's credentials to the new access point, and the new access point sends the reassociation response to the client. Only two packets pass between the client and the new access point, greatly shortening the reassociation time. The client also uses the reassociation response to generate the unicast key. Refer to the [“Configuring Fast Secure Roaming”](#) section on page 11-21 for instructions on configuring access points to support fast, secure roaming.

Understanding Radio Management

access point/bridges participating in radio management scan the radio environment and send reports to the WDS device on such radio information as potential rogue access points, associated clients, client signal strengths, and the radio signals from other access points. The WDS device forwards the aggregated radio data to the WLSE device on your network. access point/bridges participating in radio management also assist with the self-healing wireless LAN, automatically adjusting settings to provide coverage in case a nearby access point fails. Refer to the [“Configuring Radio Management”](#) section on page 11-25 for instructions on configuring radio management.

Click this URL to browse to the WLSE documentation:

http://www.cisco.com/en/US/products/sw/cscowork/ps3915/prod_technical_documentation.html

Understanding Layer 3 Mobility

When you use a WLSM as the WDS device on your network, you can install access point/bridges anywhere in a large Layer 3 network without configuring one specific subnet or VLAN throughout the wired switch infrastructure. Client devices use multipoint GRE (mGRE) tunnels to roam to access points that reside on different Layer 3 subnets. The roaming clients stay connected to your network without changing IP addresses.

For instructions on configuring WDS on a switch equipped with a Wireless LAN Services Module (WLSM), refer to the *Cisco Catalyst 6500 Series Wireless LAN Services Module (WLSM) Deployment Guide*.

The Layer 3 mobility wireless LAN solution consists of these hardware and software components:

- Access points participating in WDS
- Catalyst 6500 switch with Supervisor Module and WLSM configured as the WDS device

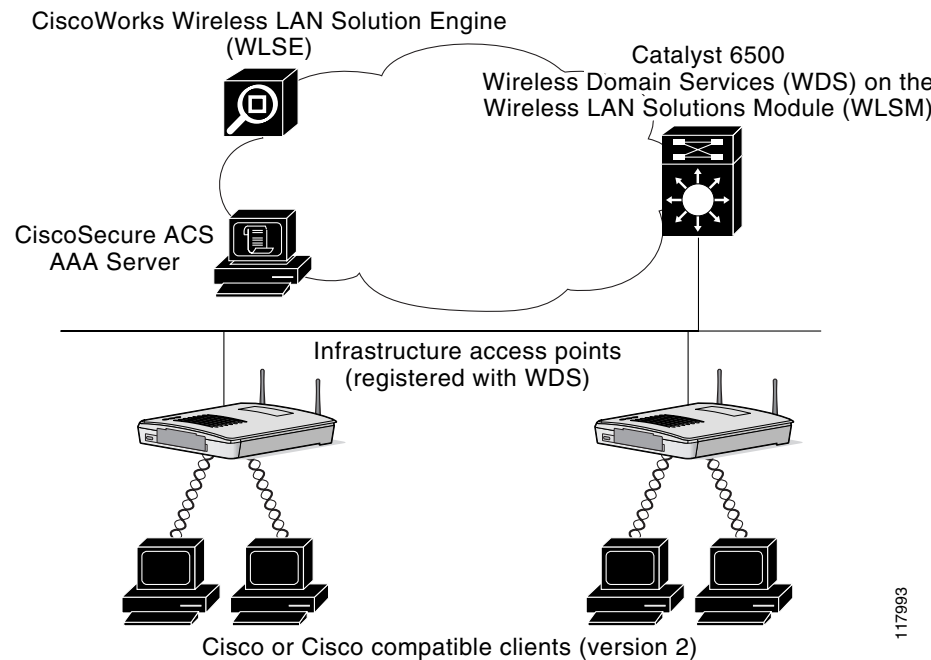
**Note**

You must use a WLSM as your WDS device to properly configure Layer 3 mobility. Layer 3 mobility is not supported when you use an access point as your WDS device.

- Client devices

Figure 11-3 shows the components that interact to perform Layer 3 mobility.

Figure 11-3 Required Components for Layer 3 Mobility



Click this link to browse to the information pages for the Cisco Structured Wireless-Aware Network (SWAN):

http://www.cisco.com/en/US/netsol/ns340/ns394/ns348/ns337/networking_solutions_package.html

**Note**

If you enable Layer 3 mobility for an SSID and your WDS device does not support Layer 3 mobility, client devices cannot associate using that SSID.

**Note**

Repeater access points and access points in workgroup bridge mode cannot associate to an SSID on which Layer 3 mobility is enabled.

Understanding Wireless Intrusion Detection Services

When you implement Wireless Intrusion Detection Services (WIDS) on your wireless LAN, your access points, WLSE, and an optional (non-Cisco) WIDS engine work together to detect and prevent attacks on your wireless LAN infrastructure and associated client devices.

Working with the WLSE, access points can detect intrusions and take action to defend the wireless LAN. WIDS consists of these features:

- Switch port tracing and rogue suppression—Switch port tracing and suppression uses an RF detection method that produces the radio MAC address of an unknown radio (a potential rogue device). The WLSE derives a wired-side MAC address from the wireless MAC address and uses it to search the switch's BRIDGE MIB. When one or more searchable MAC addresses are available, the WLSE uses CDP to discover any switches connected up to two hops away from the detecting access points. The WLSE examines the BRIDGE MIB of each CDP-discovered switch to determine if they contain any of the target MAC addresses. If CDP finds any of the MAC addresses, WLSE suppresses the corresponding switch port number.
- Excessive management frame detection—Excessive management frames indicate an attack on your wireless LAN. An attacker might carry out a denial-of-service attack by injecting excessive management frames over the radio to overwhelm access points which have to process the frames. As part of the WIDS feature set, access points in scanning mode and root access points monitor radio signals and detect excessive management frames. When they detect excessive management frames, the access points generate a fault and send it through the WDS to the WLSE.
- Authentication/protection failure detection—Authentication/protection failure detection looks for attackers who are either trying to overcome the initial authentication phase on a wireless LAN or to compromise the ongoing link protection. These detection mechanisms address specific authentication attacks:
 - EAPOL flood detection
 - MIC/encryption failures detection
 - MAC spoofing detection
- Frame capture mode—In frame capture mode, a scanner access point collects 802.11 frames and forwards them to the address of a WIDS engine on your network.

See the [“Configuring Access Points to Participate in WIDS”](#) section on page 11-27 for instructions on configuring the access point/bridge to participate in WIDS.

Configuring WDS

This section describes how to configure WDS on your network. This section contains these sections:

- [Guidelines for WDS, page 11-7](#)
- [Requirements for WDS, page 11-7](#)
- [Configuration Overview, page 11-7](#)
- [Configuring Access Point/Bridges as Potential WDS Devices, page 11-8](#)
- [Configuring Access Points to use the WDS Device, page 11-13](#)
- [Configuring the Authentication Server to Support WDS, page 11-14](#)
- [Viewing WDS Information, page 11-20](#)
- [Using Debug Messages, page 11-21](#)

Guidelines for WDS

Follow these guidelines when configuring WDS:

- A WDS access point that also serves client devices supports up to 30 participating access points, but a WDS access point with radios disabled supports up to 60 participating access points.
- Repeater access points do not support WDS. Do not configure a repeater access point as a WDS candidate, and do not configure a WDS access point to return (fall back) to repeater mode in case of Ethernet failure.

Requirements for WDS

To configure WDS, you must have these items on your wireless LAN:

- At least one access point, Integrated Services Router (ISR), or switch (equipped with a Wireless LAN Services Module) that you can configure as the WDS device
- An authentication server (or an access point or ISR configured as a local authenticator)

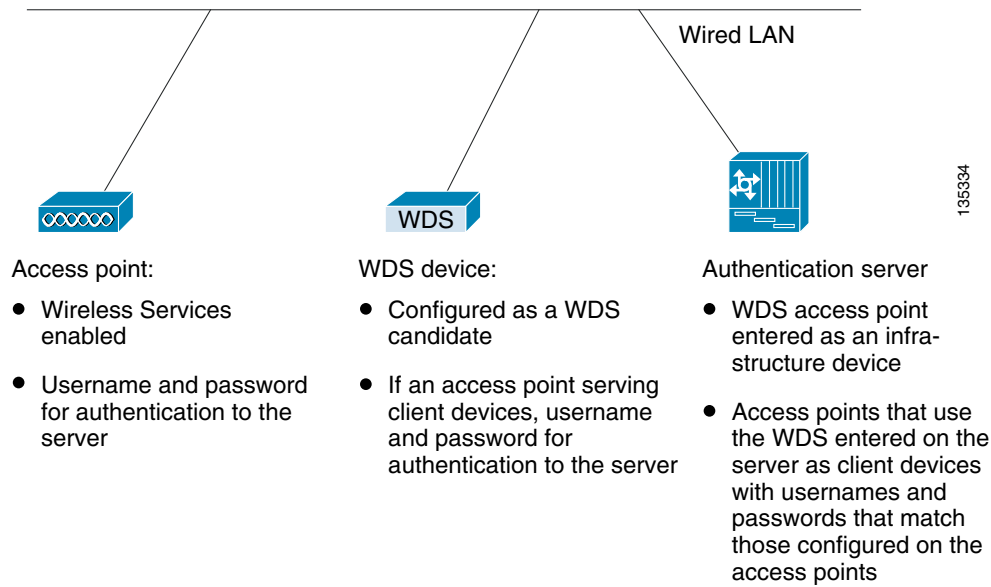
Configuration Overview

You must complete three major steps to set up WDS and fast, secure roaming:

1. Configure access points, ISRs, or switches as potential WDS devices. This chapter provides instructions for configuring an access point as a WDS device. For instructions on configuring WDS on a switch equipped with a Wireless LAN Services Module (WLSM), refer to the *Cisco Catalyst 6500 Series Wireless LAN Services Module (WLSM) Deployment Guide*.
2. Configure the rest of your access points to use the WDS device.
3. Configure the authentication server on your network to authenticate the WDS device and the access points that use the WDS device.

Figure 11-4 shows the required configuration for each device that participates in WDS.

Figure 11-4 Configurations on Devices Participating in WDS



Configuring Access Point/Bridges as Potential WDS Devices



Note

For the main WDS candidate, configure an access point/bridge that does not serve a large number of client devices. If client devices associate to the WDS access point when it starts up, the clients might wait several minutes to be authenticated.



Note

Repeater access points do not support WDS. Do not configure a repeater access point as a WDS candidate, and do not configure a WDS access point to fall back to repeater mode in case of Ethernet failure.



Note

When WDS is enabled, the WDS access point performs and tracks all authentications. Therefore, you must configure EAP security settings on the WDS access point. See [Chapter 11, “Configuring Authentication Types,”](#) for instructions on configuring EAP on the access point.

On the access point that you want to configure as your primary WDS access point, follow these steps to configure the access point as the main WDS candidate:

- Step 1** Browse to the Wireless Services Summary page. [Figure 11-5](#) shows the Wireless Services Summary page.

Figure 11-5 Wireless Services Summary Page

Wireless Services Summary				
AP				
WDS MAC Address	WDS IP Address	IN Authenticator	MN Authenticator	State

Wireless Domain Services			
MAC Address	IP Address	Priority	State

Refresh

- Step 2** Click **WDS** to browse to the WDS/WNM Summary page.

- Step 3** On the WDS/WNM Summary page, click **General Setup** to browse to the WDS/WNM General Setup page. [Figure 11-6](#) shows the General Setup page.

Figure 11-6 WDS/WNM General Setup Page

WDS STATUS SERVER GROUPS **GENERAL SET-UP**

Hostname ap ap uptime is 1 day, 21 hours, 33 minutes

Wireless Services: WDS/WNM - General Set-Up

WDS - Wireless Domain Services - Global Properties

☐ Use this AP as Wireless Domain Services

Wireless Domain Services Priority: (1-255)

☐ Use Local MAC List for Client Authentication

WNM - Wireless Network Manager - Global Configuration

☐ Configure Wireless Network Manager

Wireless Network Manager IP Address: (IP Address)

Apply Cancel

- Step 4** Check the *Use this AP as Wireless Domain Services* check box.

Step 5 In the Wireless Domain Services Priority field, enter a priority number from 1 to 255 to set the priority of this WDS candidate. The WDS access point candidate with the highest number in the priority field becomes the acting WDS access point. For example, if one WDS candidate is assigned priority 255 and one candidate is assigned priority 100, the candidate with priority 255 becomes the acting WDS access point.

Step 6 (Optional) Select the *Use Local MAC List for Client Authentication* check box to authenticate client devices using MAC addresses in the local list of addresses configured on the WDS device. If you do not select this check box, the WDS device uses the server specified for MAC-address authentication on the Server Groups page to authenticate clients based on MAC addresses.



Note Selecting the *Use Local MAC List for Client Authentication* check box does not force client devices to perform MAC-based authentication. It provides a local alternative to server-based MAC-address authentication.

Step 7 (Optional) If you use a Wireless LAN Solutions Engine (WLSE) on your network, check the *Configure Wireless Network Manager* check box and enter the IP address of the WLSE device in the *Wireless Network Manager IP Address* field. The WDS access point collects radio measurement information from access points and client devices and sends the aggregated data to the WLSE device.

Step 8 Click **Apply**.

Step 9 Click **Server Groups** to browse to the WDS Server Groups page. [Figure 11-7](#) shows the WDS Server Groups page.

Figure 11-7 WDS Server Groups Page

WDS STATUS SERVER GROUPS GENERAL SET-UP

Hostname AP1230 11:20:26 Wed May 18 2005

Wireless Services: WDS - Server Groups

Server Group List

< NEW >

infra_devices

client_devices

Delete

Server Group Name:

Group Server Priorities: [Define Servers](#)

Priority 1: < NONE >

Priority 2: < NONE >

Priority 3: < NONE >

Use Group For:

☒ Infrastructure Authentication

☐ Client Authentication

Authentication Settings

☐ EAP Authentication

☐ LEAP Authentication

☐ MAC Authentication

☐ Default (Any) Authentication

SSID Settings

☒ Apply to all SSIDs

☐ Restrict SSIDs (Apply only to listed SSIDs)

SSID: Add Remove

Apply Cancel

- Step 10** Create a group of servers to be used for 802.1x authentication for the infrastructure devices (access points) that use the WDS access point. Enter a group name in the Server Group Name field.
- Step 11** Select the primary server from the Priority 1 drop-down menu. (If a server that you need to add to the group does not appear in the Priority drop-down menus, click **Define Servers** to browse to the Server Manager page. Configure the server there, and then return to the WDS Server Groups page.)



Note If you don't have an authentication server on your network, you can configure an access point or an ISR as a local authentication server. See [Chapter 9, "Configuring an Access Point as a Local Authenticator,"](#) for configuration instructions.

- Step 12** (Optional) Select backup servers from the Priority 2 and 3 drop-down menus.
- Step 13** Click **Apply**.

- Step 14** Configure the list of servers to be used for 802.1x authentication for client devices. You can specify a separate list for clients using a certain type of authentication, such as EAP, LEAP, PEAP, or MAC-based, or specify a list for client devices using any type of authentication. Enter a group name for the server or servers in the Server Group Name field.
- Step 15** Select the primary server from the Priority 1 drop-down menu. (If a server that you need to add to the group does not appear in the Priority drop-down menus, click **Define Servers** to browse to the Server Manager page. Configure the server there, and then return to the WDS Server Groups page.)
- Step 16** (Optional) Select backup servers from the Priority 2 and 3 drop-down menus.
- Step 17** (Optional) Select **Restrict SSIDs** to limit use of the server group to client devices using specific SSIDs. Enter an SSID in the SSID field and click **Add**. To remove an SSID, highlight it in the SSID list and click **Remove**.
- Step 18** Click **Apply**.
- Step 19** Configure the WDS access point for LEAP authentication. See [Chapter 11, “Configuring Authentication Types,”](#) for instructions on configuring LEAP.

**Note**

If your WDS access point serves client devices, follow the instructions in the [“Configuring Access Points to use the WDS Device”](#) section on page 11-13 to configure the WDS access point to use the WDS.

CLI Configuration Example

This example shows the CLI commands that are equivalent to the steps listed in the [“Configuring Access Point/Bridges as Potential WDS Devices”](#) section on page 11-8:

```
AP# configure terminal
AP(config)# aaa new-model
AP(config)# wlccp wds priority 200 interface bvi1
AP(config)# wlccp authentication-server infrastructure infra_devices
AP(config)# wlccp authentication-server client any client_devices
AP(config-wlccp-auth)# ssid fred
AP(config-wlccp-auth)# ssid ginger
AP(config)# end
```

In this example, infrastructure devices are authenticated using server group *infra_devices*; client devices using SSIDs *fred* or *ginger* are authenticated using server group *client_devices*.

For complete descriptions of the commands used in this example, consult the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*.

Configuring Access Points to use the WDS Device

Follow these steps to configure an access point to authenticate through the WDS device and participate in WDS:

- Step 1** Browse to the Wireless Services Summary page.
- Step 2** Click **AP** to browse to the Wireless Services AP page. [Figure 11-8](#) shows the Wireless Services AP page.

Figure 11-8 Wireless Services AP Page

HOME
EXPRESS SET-UP
EXPRESS SECURITY
NETWORK MAP +
ASSOCIATION +
NETWORK INTERFACES +
SECURITY +
SERVICES +
WIRELESS SERVICES
AP
WDS
SYSTEM SOFTWARE +
EVENT LOG +

Hostname bridge bridge uptime is 19 hours, 27 minutes

Wireless Services: AP

Participate in SWAN Infrastructure: ☐ Enable ☒ Disable

WDS Discovery: ☒ Auto Discovery
☐ Specified Discovery: DISABLED (IP Address)

Username: DISABLED

Password: [REDACTED]

Confirm Password: [REDACTED]

L3 Mobility Service via IP/GRE Tunnel: ☐ Enable: GRE Tunnel MTU: DISABLED (256-1542)
☒ Disable

Apply Cancel

117037

- Step 3** Click **Enable** for the *Participate in SWAN Infrastructure* setting.
- Step 4** (Optional) If you use a WLSM switch module as the WDS device on your network, select **Specified Discovery** and enter the IP address of the WLSM in the entry field. When you enable Specified Discovery, the access point/bridge immediately authenticates with the WDS device instead of waiting for WDS advertisements. If the WDS device that you specify does not respond, the access point waits for WDS advertisements.
- Step 5** In the Username field, enter a username for the access point/bridge. This username must match the username that you create for the access point/bridge on your authentication server.
- Step 6** In the Password field, enter a password for the access point/bridge, and enter the password again in the Confirm Password field. This password must match the password that you create for the access point/bridge on your authentication server.
- Step 7** Click **Apply**.

The access points that you configure to interact with the WDS automatically perform these steps:

- Discover and track the current WDS device and relay WDS advertisements to the wireless LAN.
- Authenticate with the WDS device and establish a secure communication channel to the WDS device.
- Register associated client devices with the WDS device.

CLI Configuration Example

This example shows the CLI commands that are equivalent to the steps listed in the [“Configuring Access Points to use the WDS Device”](#) section on page 11-13:

```
AP# configure terminal
AP(config)# wlcgp ap username APWestWing password 7 wes7win8
AP(config)# end
```

In this example, the access point is enabled to interact with the WDS device, and it authenticates to your authentication server using *APWestWing* as its username and *wes7win8* as its password. You must configure the same username and password pair when you set up the access point as a client on your authentication server.

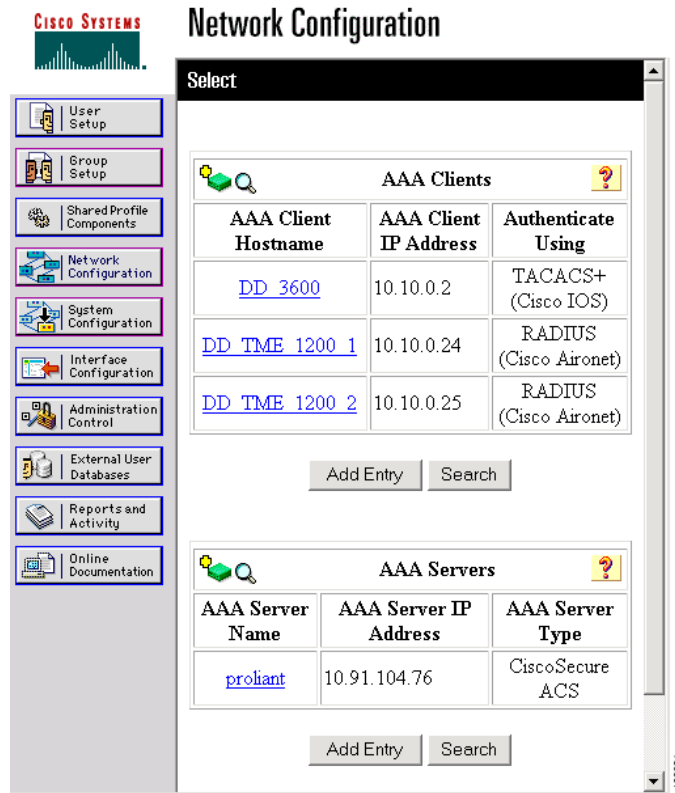
For complete descriptions of the commands used in this example, consult the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*.

Configuring the Authentication Server to Support WDS

The WDS device and all access points participating in WDS must authenticate to your authentication server. On your server, you must configure usernames and passwords for the access points and a username and password for the WDS device.

If your server runs Cisco ACS, follow these steps to configure the access points on your server:

-
- Step 1** Log into Cisco Secure ACS and click **Network Configuration** to browse to the Network Configuration page. You must use the Network Configuration page to create an entry for the WDS device. [Figure 11-9](#) shows the Network Configuration page.

Figure 11-9 Network Configuration Page


The screenshot shows the Cisco Network Configuration page. On the left is a sidebar with navigation links: User Setup, Group Setup, Shared Profile Components, Network Configuration (highlighted), System Configuration, Interface Configuration, Administration Control, External User Databases, Reports and Activity, and Online Documentation. The main content area is titled 'Network Configuration' and has a 'Select' dropdown menu. Below this are two tables: 'AAA Clients' and 'AAA Servers'. The 'AAA Clients' table has columns for AAA Client Hostname, AAA Client IP Address, and Authenticate Using. It lists three entries: 'DD 3600' with IP 10.10.0.2 using TACACS+ (Cisco IOS), 'DD TME 1200 1' with IP 10.10.0.24 using RADIUS (Cisco Aironet), and 'DD TME 1200 2' with IP 10.10.0.25 using RADIUS (Cisco Aironet). The 'AAA Servers' table has columns for AAA Server Name, AAA Server IP Address, and AAA Server Type. It lists one entry: 'proliant' with IP 10.91.104.76 using CiscoSecure ACS. Both tables have 'Add Entry' and 'Search' buttons below them.

AAA Client Hostname	AAA Client IP Address	Authenticate Using
DD 3600	10.10.0.2	TACACS+ (Cisco IOS)
DD TME 1200 1	10.10.0.24	RADIUS (Cisco Aironet)
DD TME 1200 2	10.10.0.25	RADIUS (Cisco Aironet)

AAA Server Name	AAA Server IP Address	AAA Server Type
proliant	10.91.104.76	CiscoSecure ACS

Step 2 Click **Add Entry** under the AAA Clients table. The Add AAA Client page appears. [Figure 11-10](#) shows the Add AAA Client page.

Figure 11-10 Add AAA Client Page

CISCO SYSTEMS

Network Configuration

Edit

Add AAA Client

AAA Client Hostname: APSouthside

AAA Client IP Address: 10.91.104.99

Key: password

Authenticate Using: RADIUS (Cisco Aironet)

☐ Single Connect TACACS+ AAA Client (Record stop in accounting on failure).
☐ Log Update/Watchdog Packets from this AAA Client
☐ Log RADIUS Tunneling Packets from this AAA Client
☐ Replace RADIUS Port info with Username from this AAA Client

Submit Submit + Restart Cancel

- Step 3** In the AAA Client Hostname field, enter the name of the WDS device.
- Step 4** In the AAA Client IP Address field, enter the IP address of the WDS device.
- Step 5** In the Key field, enter exactly the same password that is configured on the WDS device.
- Step 6** From the Authenticate Using drop-down menu, select **RADIUS (Cisco Aironet)**.
- Step 7** Click **Submit**.
- Step 8** Repeat [Step 2](#) through [Step 7](#) for each WDS device candidate.
- Step 9** Click **User Setup** to browse to the User Setup page. You must use the User Setup page to create entries for the access points that use the WDS device. [Figure 11-11](#) shows the User Setup page.

Figure 11-11 User Setup Page

CISCO SYSTEMS

User Setup

Select

User:

List users beginning with letter/number:

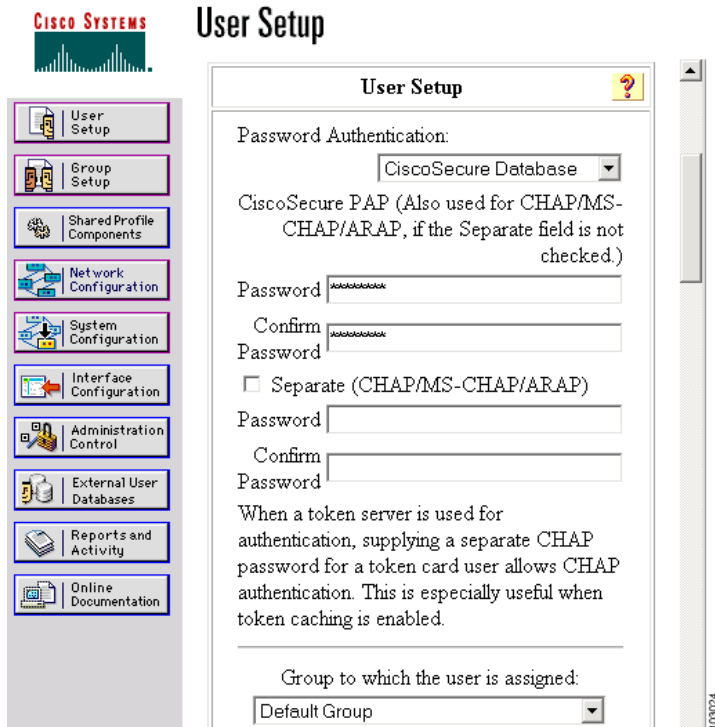
[A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#)
[N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [X](#) [Y](#) [Z](#)
[0](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#)

103023

Step 10 Enter the name of the access point in the User field.

Step 11 Click **Add/Edit**.

Step 12 Scroll down to the User Setup box. [Figure 11-12](#) shows the User Setup box.

Figure 11-12 ACS User Setup Box


CISCO SYSTEMS

User Setup

User Setup

Group Setup

Shared Profile Components

Network Configuration

System Configuration

Interface Configuration

Administration Control

External User Databases

Reports and Activity

Online Documentation

User Setup

Password Authentication:
CiscoSecure Database

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password

Confirm Password

☐ Separate (CHAP/MS-CHAP/ARAP)

Password

Confirm Password

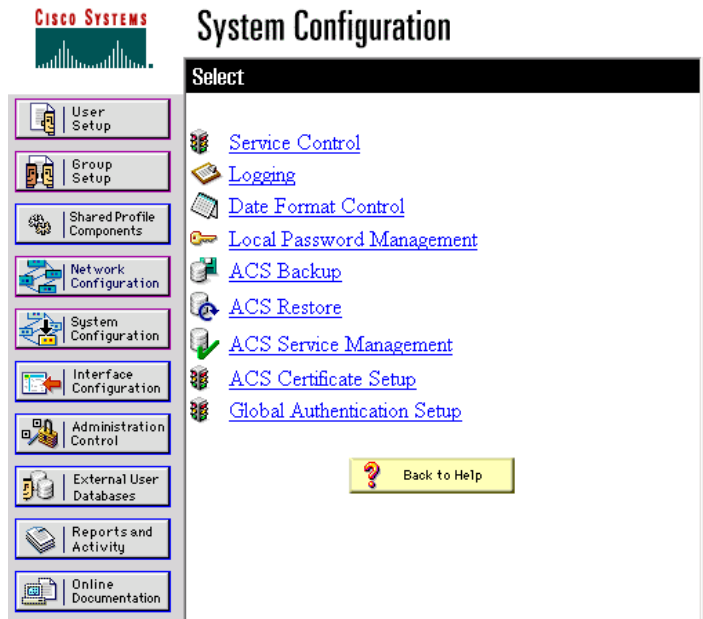
When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

Group to which the user is assigned:
Default Group

- Step 13** Select **CiscoSecure Database** from the Password Authentication drop-down menu.
- Step 14** In the Password and Confirm Password fields, enter exactly the same password that you entered on the access point on the Wireless Services AP page.
- Step 15** Click **Submit**.
- Step 16** Repeat [Step 10](#) through [Step 15](#) for each access point that uses the WDS device.

- Step 17** Browse to the System Configuration page, click **Service Control**, and restart ACS to apply your entries. [Figure 11-13](#) shows the System Configuration page.

Figure 11-13 ACS System Configuration Page



Viewing WDS Information

On the web-browser interface, browse to the Wireless Services Summary page to view a summary of WDS status.

On the CLI in privileged exec mode, use these commands to view information about the current WDS device and other access points participating in CCKM:

Command	Description
show wlccp ap	Use this command on access points participating in CCKM to display the WDS device's MAC address, the WDS device's IP address, the access point/bridge's state (authenticating, authenticated, or registered), the IP address of the infrastructure authenticator, and the IP address of the client device (MN) authenticator.
show wlccp wds { ap mn } [detail] [mac-addr <i>mac-address</i>]	On the WDS device only, use this command to display cached information about access points and client devices. • ap—Use this option to display access points participating in CCKM. The command displays each access point's MAC address, IP address, state (authenticating, authenticated, or registered), and lifetime (seconds remaining before the access point must reauthenticate). Use the mac-addr option to display information about a specific access point. • mn—Use this option to display cached information about client devices, also called mobile nodes. The command displays each client's MAC address, IP address, the access point to which the client is associated (cur-AP), and state (authenticating, authenticated, or registered). Use the detail option to display the client's lifetime (seconds remaining before the client must reauthenticate), SSID, and VLAN ID. Use the mac-addr option to display information about a specific client device. If you only enter show wlccp wds, the command displays the access point/bridge's IP address, MAC address, priority, and interface state (administratively standalone, active, backup, or candidate). If the state is backup, the command also displays the current WDS device's IP address, MAC address, and priority.

Using Debug Messages

In privileged exec mode, use these debug commands to control the display of debug messages for devices interacting with the WDS device:

Command	Description
debug wlccp ap { mn wds-discovery state }	Use this command to turn on display of debug messages related to client devices (mn), the WDS discovery process, and access point authentication to the WDS device (state).
debug wlccp dump	Use this command to perform a dump of WLCCP packets received and sent in binary format.
debug wlccp packet	Use this command to turn on display of packets to and from the WDS device.
debug wlccp wds [aggregator authenticator nm state statistics]	Use this command and its options to turn on display of WDS debug messages. Use the statistics option to turn on display of failure statistics.
debug wlccp wds authenticator { all dispatcher mac-authen process rxdata state-machine txdata }	Use this command and its options to turn on display of WDS debug messages related to authentication.

Configuring Fast Secure Roaming

After you configure WDS, access points configured for CCKM can provide fast, secure roaming for associated client devices. This section describes how to configure fast, secure roaming on your wireless LAN. This section contains these sections:

- [Requirements for Fast Secure Roaming](#)
- [Configuring Access Points to Support Fast Secure Roaming](#)

Requirements for Fast Secure Roaming

To configure fast secure roaming, you must have these items on your wireless LAN:

- At least one access point, ISR, or switch (equipped with a WLSM) configured as the WDS device
- Access points configured to participate in WDS
- Access points configured for fast, secure roaming
- An authentication server (or an access point, ISR, or switch configured as a local authenticator)
- Cisco Aironet client devices, or Cisco-compatible client devices that comply with Cisco Compatible Extensions (CCX) version 2 or later

For instructions on configuring WDS, refer to the [“Configuring WDS” section on page 11-6](#).

Configuring Access Points to Support Fast Secure Roaming

To support fast, secure roaming, the access points on your wireless LAN must be configured to participate in WDS and they must allow CCKM authenticated key management for at least one SSID. Follow these steps to configure CCKM for an SSID:

- Step 1** Browse to the Encryption Manager page on the access point GUI. [Figure 11-14](#) shows the top section of the Encryption Manager page.

Figure 11-14 Encryption Manager Page

HOME | RADIO0-802.11G | RADIO1-802.11A

Hostname AP1230 16:25:05 Wed May 18 2005

Security: Encryption Manager - Radio0.802.11G

Encryption Modes

☐ None

☐ WEP Encryption Optional

Cisco Compliant TKIP Features: ☐ Enable Message Integrity Check (MIC)

☐ Enable Per Packet Keying (PPK)

☒ Cipher CKIP + CMIC

135383

- Step 2** Click the **Cipher** button.
- Step 3** Select **CKIP + CMIC** from the Cipher drop-down menu.
- Step 4** Click **Apply**.
- Step 5** Browse to the Global SSID Manager page. [Figure 11-15](#) shows the top sections of the Global SSID Manager page.

Figure 11-15 Global SSID Manager Page

HOME Hostname AP1230 08:05:20 Thu May 19 2005

EXPRESS SET-UP

EXPRESS SECURITY

NETWORK MAP +

ASSOCIATION +

NETWORK INTERFACES +

SECURITY

Admin Access

Encryption Manager

SSID Manager

Server Manager

Local RADIUS Server

Advanced Security

SERVICES +

WIRELESS SERVICES +

SYSTEM SOFTWARE +

EVENT LOG +

Security: Global SSID Manager

SSID Properties

Current SSID List

< NEW >
UC
fastroam

SSID: fastroam

VLAN: < NONE > [Define VLANs](#)

Interface: ☒ Radio0-802.11G
☐ Radio1-802.11A

Network ID: (0-4096)

Delete

Authentication Settings

Methods Accepted:

☐ Open Authentication: < NO ADDITION >

☐ Shared Authentication: < NO ADDITION >

☒ Network EAP: < NO ADDITION >

Server Priorities:

EAP Authentication Servers

☒ Use Defaults [Define Defaults](#)

☐ Customize

Priority 1: < NONE >

Priority 2: < NONE >

Priority 3: < NONE >

MAC Authentication Servers

☒ Use Defaults [Define Defaults](#)

☐ Customize

Priority 1: < NONE >

Priority 2: < NONE >

Priority 3: < NONE >

Authenticated Key Management

Key Management: Mandatory ☒ CCKM ☐ WPA

WPA Pre-shared Key: ☒ ASCII ☐ Hexadecimal

135384

Step 6 On the SSID that supports CCKM, select these settings:

- b. If your access point contains multiple radio interfaces, select the interfaces on which the SSID applies.
- c. Select **Network EAP** under Authentication Settings. When you enable CCKM, you must enable Network EAP as the authentication type.

- d. Select **Mandatory** or **Optional** under Authenticated Key Management. If you select **Mandatory**, only clients that support CCKM can associate using the SSID. If you select **Optional**, both CCKM clients and clients that do not support CCKM can associate using the SSID.
- e. Check the **CCKM** check box.

Step 7 Click **Apply**.

CLI Configuration Example

This example shows the CLI commands that are equivalent to the steps listed in the “[Configuring Access Points to Support Fast Secure Roaming](#)” section on page 11-22:

```
AP# configure terminal
AP(config)# dot11 ssid fastroam
AP(config-ssid)# authentication network-eap eap_methods
AP(config-ssid)# authentication key-management cckm
AP(config-ssid)# exit
AP(config)# interface dot11radio0
AP(config-if)# encryption mode ciphers ckip-cmic
AP(config-if)# ssid fastroam
AP(config-if)# exit
AP(config)# end
```

In this example, the SSID *fastroam* is configured to support Network EAP and CCKM, the CKIP-CMIC cipher suite is enabled on the 2.4-GHz radio interface, and the SSID *fastroam* is enabled on the 2.4-GHz radio interface.

For complete descriptions of the commands used in this example, consult the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*.

Configuring Radio Management

When you configure access points on your wireless LAN to use WDS, the access points automatically play a role in radio management when they interact with the WDS device. To complete the radio management configuration, you configure the WDS device to interact with the WLSE device on your network.

Follow these steps to enable radio management on an access point configured as a WDS device:

- Step 1** Browse to the Wireless Services Summary page. [Figure 11-16](#) shows the Wireless Services Summary page.

Figure 11-16 Wireless Services Summary Page

Wireless Services Summary				
AP				
WDS MAC Address	WDS IP Address	IN Authenticator	MN Authenticator	State

Wireless Domain Services			
MAC Address	IP Address	Priority	State

Refresh

- Step 2** Click **WDS** to browse to the General Setup page.
- Step 3** On the WDS/WNM Summary page, click **Settings** to browse to the General Setup page. [Figure 11-17](#) shows the General Setup page.

Figure 11-17 WDS/WNM General Setup Page

- Step 4** Check the *Configure Wireless Network Manager* check box.
- Step 5** In the *Wireless Network Manager IP Address* field, enter the IP address of the WLSE device on your network.
- Step 6** Click **Apply**. The WDS access point is configured to interact with your WLSE device.

CLI Configuration Example

This example shows the CLI commands that are equivalent to the steps listed in the [“Configuring Radio Management” section on page 11-25](#):

```
AP# configure terminal
AP(config)# wlccp wnm ip address 192.250.0.5
AP(config)# end
```

In this example, the WDS access point is enabled to interact with a WLSE device with the IP address 192.250.0.5.

For complete descriptions of the commands used in this example, consult the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*.

Configuring Access Points to Participate in WIDS

To participate in WIDS, access points must be configured to participate in WDS and in radio management. Follow the steps in the [“Configuring Access Points to use the WDS Device” section on page 11-13](#) and in the [“Configuring Radio Management” section on page 11-25](#) to configure the access point to participate in WDS and in radio management.

Configuring the Access Point for Scanner Mode

In scanner mode, the access point scans all of its channels for radio activity and reports the activity to the WDS device on your network. A scanner access point does not accept client associations.

Beginning in privileged EXEC mode, follow these steps to set the access point radio network role to scanner:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.
Step 3	station-role scanner	Set the access point role to scanner.
Step 4	end	Return to privileged EXEC mode.

Configuring the Access Point for Monitor Mode

When an access point is configured as a scanner it can also capture frames in monitor mode. In monitor mode, the access point captures 802.11 frames and forwards them to the WIDS engine on your network. The access point adds a 28-byte capture header to every 802.11 frame that it forwards, and the WIDS engine on your network uses the header information for analysis. The access point uses UDP packets to forward captured frames. Multiple captured frames can be combined into one UDP packet to conserve network bandwidth.

In scanner mode the access point scans all channels for radio activity. However, in monitor mode the access point monitors only the channel for which the access point radio is configured.



Note

If your access point contains two radios, both radios must be configured for scanner mode before you can configure monitor mode on the interfaces.

Beginning in privileged EXEC mode, follow these steps to configure the access point to capture and forward 802.11 frames:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.

	Command	Purpose
Step 3	monitor frames endpoint ip address <i>IP-address</i> port <i>UDP-port</i> [truncate <i>truncation-length</i>]	Configure the radio for monitor mode. Enter the IP address and the UDP port on the WIDS engine on your network. (Optional) Configure a maximum length in bytes for each forwarded frame. The access point truncates frames longer than this value. The default length is 128 bytes.
Step 4	end	Return to privileged EXEC mode.

Displaying Monitor Mode Statistics

Use the **show wlccp ap rm monitor statistics** global configuration command to display statistics on captured frames.

This example shows output from the command:

```
ap# show wlccp ap rm monitor statistics

Dot11Radio 0
=====
WLAN Monitoring           : Enabled
Endpoint IP address      : 10.91.107.19
Endpoint port            : 2000
Frame Truncation Length  : 535 bytes

WLAN Monitor Statistics
=====
Total No. of frames rx by DOT11 driver      : 58475
Total No. of Dot11 no buffers               : 361
Total No. of Frames Q Failed                : 0
Current No. of frames in SCAN Q             : 0

Total No. of frames captured                 : 0
Total No. of data frames captured            : 425
Total No. of control frames captured         : 1957
Total No. of Mgmt frames captured            : 20287
Total No. of CRC errored frames captured     : 0

Total No. of captured frames forwarded      : 23179
Total No. of captured frames forward failed : 0
```

Use the **clear wlccp ap rm statistics** command to clear the monitor mode statistics.

Configuring Monitor Mode Limits

You can configure threshold values that the access point/bridge uses in monitor mode. When a threshold value is exceeded, the access point/bridge logs the information or sends an alert.

Configuring an Authentication Failure Limit

Setting an authentication failure limit protects your network against a denial-of-service attack called *EAPOL flooding*. The 802.1X authentication that takes place between a client and the access point/bridge triggers a series of messages between the access point/bridge, the authenticator, and an

authentication server using EAPOL messaging. The authentication server, typically a RADIUS server, can quickly become overwhelmed if there are too many authentication attempts. If not regulated, a single client can trigger enough authentication requests to impact your network.

In monitor mode the access point/bridge tracks the rate at which 802.1X clients attempt to authenticate through the access point/bridge. If your network is attacked through excessive authentication attempts, the access point/bridge generates an alert when the authentication threshold has been exceeded.

You can configure these limits on the access point/bridge:

- Number of 802.1X attempts through the access point/bridge
- EAPOL flood duration in seconds on the access point/bridge

When the access point/bridge detects excessive authentication attempts it sets MIB variables to indicate this information:

- An EAPOL flood was detected
- Number of authentication attempts
- MAC address of the client with the most authentication attempts

Beginning in privileged EXEC mode, follow these steps to set authentication limits that trigger a fault on the access point/bridge:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	dot11 ids eap attempts <i>number</i> period <i>seconds</i>	Configure the number of authentication attempts and the number of seconds of EAPOL flooding that trigger a fault on the access point/bridge.
Step 3	end	Return to privileged EXEC mode.



Configuring RADIUS and TACACS+ Servers

This chapter describes how to enable and configure the Remote Authentication Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+), that provides detailed accounting information and flexible administrative control over authentication and authorization processes. RADIUS and TACACS+ are facilitated through AAA and can be enabled only through AAA commands.



Note

You can configure your access point/bridge as a local authenticator to provide a backup for your main server or to provide authentication service on a network without a RADIUS server. See [Chapter 11, “Configuring Authentication Types,”](#) for detailed instructions on configuring your access point/bridge as a local authenticator.



Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Cisco IOS Security Command Reference for Release 12.2*.

This chapter contains these sections:

- [Configuring and Enabling RADIUS, page 12-2](#)
- [Configuring and Enabling TACACS+, page 12-21](#)

Configuring and Enabling RADIUS

This section describes how to configure and enable RADIUS. These sections describe RADIUS configuration:

- [Understanding RADIUS, page 12-2](#)
- [RADIUS Operation, page 12-3](#)
- [Configuring RADIUS, page 12-4](#)
- [Displaying the RADIUS Configuration, page 12-17](#)
- [RADIUS Attributes Sent by the Access Point/Bridge, page 12-18](#)

Understanding RADIUS

RADIUS is a distributed client/server system that secures networks against unauthorized access. RADIUS clients run on supported Cisco devices and send authentication requests to a central RADIUS server, which contains all user authentication and network service access information. The RADIUS host is normally a multiuser system running RADIUS server software from Cisco (Cisco Secure Access Control Server version 3.0), Livingston, Merit, Microsoft, or another software provider. For more information, refer to the RADIUS server documentation.

Use RADIUS in these network environments, which require access security:

- Networks with multiple-vendor access servers, each supporting RADIUS. For example, access servers from several vendors use a single RADIUS server-based security database. In an IP-based network with multiple vendors' access servers, dial-in users are authenticated through a RADIUS server that is customized to work with the Kerberos security system.
- Turnkey network security environments in which applications support the RADIUS protocol, such as an access environment that uses a *smart card* access control system. In one case, RADIUS has been used with Enigma's security cards to validate users and to grant access to network resources.
- Networks already using RADIUS. You can add a Cisco access point/bridge containing a RADIUS client to the network.
- Networks that require resource accounting. You can use RADIUS accounting independently of RADIUS authentication or authorization. The RADIUS accounting functions allow data to be sent at the start and end of services, showing the amount of resources (such as time, packets, bytes, and so forth) used during the session. An Internet service provider might use a freeware-based version of RADIUS access control and accounting software to meet special security and billing needs.

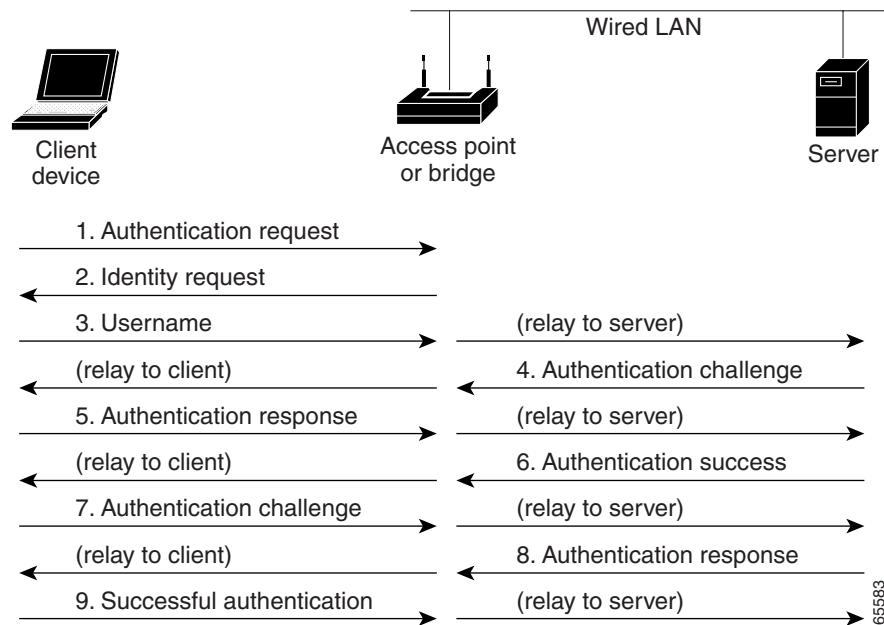
RADIUS is not suitable in these network security situations:

- Multiprotocol access environments. RADIUS does not support AppleTalk Remote Access (ARA), NetBIOS Frame Control Protocol (NBFCP), NetWare Asynchronous Services Interface (NASI), or X.25 PAD connections.
- Switch-to-switch or router-to-router situations. RADIUS does not provide two-way authentication. RADIUS can be used to authenticate from one device to a non-Cisco device if the non-Cisco device requires authentication.
- Networks using a variety of services. RADIUS generally binds a user to one service model.

RADIUS Operation

When a wireless user attempts to log in and authenticate to an access point or bridge whose access is controlled by a RADIUS server, authentication to the network occurs in the steps shown in [Figure 12-1](#):

Figure 12-1 Sequence for EAP Authentication



In Steps 1 through 9 in [Figure 12-1](#), 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/bridge. 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/bridge. The access point/bridge 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/bridge 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/bridge 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 [“Assigning Authentication Types to an SSID”](#) section on page 11-10 for instructions on setting up client authentication using a RADIUS server.

Configuring RADIUS

This section describes how to configure your access point/bridge to support RADIUS. At a minimum, you must identify the host or hosts that run the RADIUS server software and define the method lists for RADIUS authentication. You can optionally define method lists for RADIUS authorization and accounting.

A method list defines the sequence and methods to be used to authenticate, to authorize, or to keep accounts on a user. You can use method lists to designate one or more security protocols to be used, thus ensuring a backup system if the initial method fails. The software uses the first method listed to authenticate, to authorize, or to keep accounts on users; if that method does not respond, the software selects the next method in the list. This process continues until there is successful communication with a listed method or the method list is exhausted.

You should have access to and should configure a RADIUS server before configuring RADIUS features on your access point/bridge.

This section contains this configuration information:

- [Default RADIUS Configuration, page 12-4](#)
- [Identifying the RADIUS Server Host, page 12-5](#) (required)
- [Configuring RADIUS Login Authentication, page 12-7](#) (required)
- [Defining AAA Server Groups, page 12-9](#) (optional)
- [Configuring RADIUS Authorization for User Privileged Access and Network Services, page 12-11](#) (optional)
- [Starting RADIUS Accounting, page 12-12](#) (optional)
- [Selecting the CSID Format, page 12-13](#) (optional)
- [Configuring Settings for All RADIUS Servers, page 12-13](#) (optional)
- [Configuring the Access Point/Bridge to Use Vendor-Specific RADIUS Attributes, page 12-14](#) (optional)
- [Configuring the Access Point/Bridge for Vendor-Proprietary RADIUS Server Communication, page 12-15](#) (optional)
- [Configuring WISPr RADIUS Attributes, page 12-16](#) (optional)

**Note**

The RADIUS server CLI commands are disabled until you enter the **aaa new-model** command.

Default RADIUS Configuration

RADIUS and AAA are disabled by default.

To prevent a lapse in security, you cannot configure RADIUS through a network management application. When enabled, RADIUS can authenticate users accessing the access point/bridge through the CLI.

Identifying the RADIUS Server Host

Access point-to-RADIUS-server communication involves several components:

- Host name or IP address
- Authentication destination port
- Accounting destination port
- Key string
- Timeout period
- Retransmission value

You identify RADIUS security servers by their host name or IP address, host name and specific UDP port numbers, or their IP address and specific UDP port numbers. The combination of the IP address and the UDP port number creates a unique identifier allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. This unique identifier enables RADIUS requests to be sent to multiple UDP ports on a server at the same IP address.

**Note**

For Cisco IOS Releases 12.2(8)JA and later, the access point/bridge uses a randomly chosen UDP source port number in the range of 21645 to 21844 for communication with RADIUS servers.

If two different host entries on the same RADIUS server are configured for the same service—such as accounting—the second host entry configured acts as a fail-over backup to the first one. Using this example, if the first host entry fails to provide accounting services, the access point/bridge tries the second host entry configured on the same device for accounting services. (The RADIUS host entries are tried in the order that they are configured.)

A RADIUS server and the access point/bridge use a shared secret text string to encrypt passwords and exchange responses. To configure RADIUS to use the AAA security commands, you must specify the host running the RADIUS server daemon and a secret text (key) string that it shares with the access point/bridge.

The timeout, retransmission, and encryption key values can be configured globally per server for all RADIUS servers or in some combination of global and per-server settings. To apply these settings globally to all RADIUS servers communicating with the access point/bridge, use the three unique global configuration commands: **radius-server timeout**, **radius-server retransmit**, and **radius-server key**. To apply these values on a specific RADIUS server, use the **radius-server host** global configuration command.

**Note**

If you configure both global and per-server functions (timeout, retransmission, and key commands) on the access point/bridge, the per-server timer, retransmission, and key value commands override global timer, retransmission, and key value commands. For information on configuring these setting on all RADIUS servers, see the [“Configuring Settings for All RADIUS Servers” section on page 12-13](#).

You can configure the access point/bridge to use AAA server groups to group existing server hosts for authentication. For more information, see the [“Defining AAA Server Groups” section on page 12-9](#).

Beginning in privileged EXEC mode, follow these steps to configure per-server RADIUS server communication. This procedure is required.

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	aaa new-model	Enable AAA.
Step 3	radius-server host { <i>hostname</i> <i>ip-address</i> } [auth-port <i>port-number</i>] [acct-port <i>port-number</i>] [timeout <i>seconds</i>] [retransmit <i>retries</i>] [key <i>string</i>]	Specify the IP address or host name of the remote RADIUS server host. (Optional) For auth-port <i>port-number</i>, specify the UDP destination port for authentication requests. (Optional) For acct-port <i>port-number</i>, specify the UDP destination port for accounting requests. (Optional) For timeout <i>seconds</i>, specify the time interval that the access point/bridge waits for the RADIUS server to reply before retransmitting. The range is 1 to 1000. This setting overrides the radius-server timeout global configuration command setting. If no timeout is set with the radius-server host command, the setting of the radius-server timeout command is used. (Optional) For retransmit <i>retries</i>, specify the number of times a RADIUS request is resent to a server if that server is not responding or responding slowly. The range is 1 to 1000. If no retransmit value is set with the radius-server host command, the setting of the radius-server retransmit global configuration command is used. (Optional) For key <i>string</i>, specify the authentication and encryption key used between the access point/bridge and the RADIUS daemon running on the RADIUS server. Note The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the radius-server host command. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key. To configure the access point/bridge to recognize more than one host entry associated with a single IP address, enter this command as many times as necessary, making sure that each UDP port number is different. The access point/bridge software searches for hosts in the order in which you specify them. Set the timeout, retransmit, and encryption key values to use with the specific RADIUS host.
Step 4	dot11 ssid <i>ssid-string</i>	Enter SSID configuration mode for an SSID on which you need to enable accounting. The SSID can consist of up to 32 alphanumeric characters. SSIDs are case sensitive.

	Command	Purpose
Step 5	accounting <i>list-name</i>	Enable RADIUS accounting for this SSID. For <i>list-name</i>, specify the accounting method list. Click this URL for more information on method lists: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgr/fsecur_c/fsaaa/scfacct.htm#xtocid2 Note To enable accounting for an SSID, you must include the accounting command in the SSID configuration. Click this URL to browse to a detailed description of the SSID configuration mode accounting command: http://www.cisco.com/en/US/products/hw/wireless/ps4570/products_command_reference_chapter09186a008041757f.html#wp2449819
Step 6	end	Return to privileged EXEC mode.
Step 7	show running-config	Verify your entries.
Step 8	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To remove the specified RADIUS server, use the **no radius-server host** *hostname* | *ip-address* global configuration command.

This example shows how to configure one RADIUS server to be used for authentication and another to be used for accounting:

```
AP(config)# radius-server host 172.29.36.49 auth-port 1612 key rad1
AP(config)# radius-server host 172.20.36.50 acct-port 1618 key rad2
```

This example shows how to configure an SSID for RADIUS accounting:

```
AP(config)# dot11 ssid batman
AP(config-ssid)# accounting accounting-method-list
```

This example shows how to configure *host1* as the RADIUS server and to use the default ports for both authentication and accounting:

```
AP(config)# radius-server host host1
```



Note

You also need to configure some settings on the RADIUS server. These settings include the IP address of the access point/bridge and the key string to be shared by both the server and the access point/bridge. For more information, refer to the RADIUS server documentation.

Configuring RADIUS Login Authentication

To configure AAA authentication, you define a named list of authentication methods and then apply that list to various interfaces. The method list defines the types of authentication to be performed and the sequence in which they are performed; it must be applied to a specific interface before any of the defined authentication methods are performed. The only exception is the default method list (which, by coincidence, is named *default*). The default method list is automatically applied to all interfaces except those that have a named method list explicitly defined.

A method list describes the sequence and authentication methods to be queried to authenticate a user. You can designate one or more security protocols to be used for authentication, thus ensuring a backup system for authentication in case the initial method fails. The software uses the first method listed to authenticate users; if that method fails to respond, the software selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this cycle—meaning that the security server or local username database responds by denying the user access—the authentication process stops, and no other authentication methods are attempted.

Beginning in privileged EXEC mode, follow these steps to configure login authentication. This procedure is required.

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	aaa new-model	Enable AAA.
Step 3	aaa authentication login {default list-name} method1 [method2...]	Create a login authentication method list. - To create a default list that is used when a named list is <i>not</i> specified in the login authentication command, use the default keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all interfaces. For more information on list names, click this link: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fsaaa/scfathen.htm#xtocid2 - For <i>method1...</i>, specify the actual method the authentication algorithm tries. The additional methods of authentication are used only if the previous method returns an error, not if it fails. Select one of these methods: line—Use the line password for authentication. You must define a line password before you can use this authentication method. Use the password password line configuration command. local—Use the local username database for authentication. You must enter username information in the database. Use the username password global configuration command. radius—Use RADIUS authentication. You must configure the RADIUS server before you can use this authentication method. For more information, see the “Identifying the RADIUS Server Host” section on page 12-5.
Step 4	line [console tty vty] line-number [ending-line-number]	Enter line configuration mode, and configure the lines to which you want to apply the authentication list.
Step 5	login authentication {default list-name}	Apply the authentication list to a line or set of lines. - If you specify default, use the default list created with the aaa authentication login command. - For <i>list-name</i>, specify the list created with the aaa authentication login command.
Step 6	radius-server attribute 32 include-in-access-req format %h	Configure the access point/bridge to send its system name in the NAS_ID attribute for authentication.
Step 7	end	Return to privileged EXEC mode.

	Command	Purpose
Step 8	show running-config	Verify your entries.
Step 9	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To disable AAA, use the **no aaa new-model** global configuration command. To disable AAA authentication, use the **no aaa authentication login {default | list-name} method1 [method2...]** global configuration command. To either disable RADIUS authentication for logins or to return to the default value, use the **no login authentication {default | list-name}** line configuration command.

Defining AAA Server Groups

You can configure the access point/bridge to use AAA server groups to group existing server hosts for authentication. You select a subset of the configured server hosts and use them for a particular service. The server group is used with a global server-host list, which lists the IP addresses of the selected server hosts.

Server groups also can include multiple host entries for the same server if each entry has a unique identifier (the combination of the IP address and UDP port number), allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. If you configure two different host entries on the same RADIUS server for the same service (such as accounting), the second configured host entry acts as a fail-over backup to the first one.

You use the **server** group server configuration command to associate a particular server with a defined group server. You can either identify the server by its IP address or identify multiple host instances or entries by using the optional **auth-port** and **acct-port** keywords.

Beginning in privileged EXEC mode, follow these steps to define the AAA server group and associate a particular RADIUS server with it:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	aaa new-model	Enable AAA.

	Command	Purpose
Step 3	radius-server host { <i>hostname</i> <i>ip-address</i> } [auth-port <i>port-number</i>] [acct-port <i>port-number</i>] [timeout <i>seconds</i>] [retransmit <i>retries</i>] [key <i>string</i>]	Specify the IP address or host name of the remote RADIUS server host. • (Optional) For auth-port <i>port-number</i>, specify the UDP destination port for authentication requests. • (Optional) For acct-port <i>port-number</i>, specify the UDP destination port for accounting requests. • (Optional) For timeout <i>seconds</i>, specify the time interval that the access point/bridge waits for the RADIUS server to reply before retransmitting. The range is 1 to 1000. This setting overrides the radius-server timeout global configuration command setting. If no timeout is set with the radius-server host command, the setting of the radius-server timeout command is used. • (Optional) For retransmit <i>retries</i>, specify the number of times a RADIUS request is resent to a server if that server is not responding or responding slowly. The range is 1 to 1000. If no retransmit value is set with the radius-server host command, the setting of the radius-server retransmit global configuration command is used. • (Optional) For key <i>string</i>, specify the authentication and encryption key used between the access point/bridge and the RADIUS daemon running on the RADIUS server. Note The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the radius-server host command. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key. To configure the access point/bridge to recognize more than one host entry associated with a single IP address, enter this command as many times as necessary, making sure that each UDP port number is different. The access point/bridge software searches for hosts in the order in which you specify them. Set the timeout, retransmit, and encryption key values to use with the specific RADIUS host.
Step 4	aaa group server radius <i>group-name</i>	Define the AAA server-group with a group name. This command puts the access point/bridge in a server group configuration mode.
Step 5	server <i>ip-address</i>	Associate a particular RADIUS server with the defined server group. Repeat this step for each RADIUS server in the AAA server group. Each server in the group must be previously defined in Step 2.
Step 6	end	Return to privileged EXEC mode.
Step 7	show running-config	Verify your entries.
Step 8	copy running-config startup-config	(Optional) Save your entries in the configuration file.
Step 9		Enable RADIUS login authentication. See the “Configuring RADIUS Login Authentication” section on page 12-7.

To remove the specified RADIUS server, use the **no radius-server host** *hostname* | *ip-address* global configuration command. To remove a server group from the configuration list, use the **no aaa group server radius** *group-name* global configuration command. To remove the IP address of a RADIUS server, use the **no server ip-address** server group configuration command.

In this example, the access point/bridge is configured to recognize two different RADIUS group servers (*group1* and *group2*). Group1 has two different host entries on the same RADIUS server configured for the same services. The second host entry acts as a fail-over backup to the first entry.

```
AP(config)# aaa new-model
AP(config)# radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
AP(config)# radius-server host 172.10.0.1 auth-port 1645 acct-port 1646
AP(config)# aaa group server radius group1
AP(config-sg-radius)# server 172.20.0.1 auth-port 1000 acct-port 1001
AP(config-sg-radius)# exit
AP(config)# aaa group server radius group2
AP(config-sg-radius)# server 172.20.0.1 auth-port 2000 acct-port 2001
AP(config-sg-radius)# exit
```

Configuring RADIUS Authorization for User Privileged Access and Network Services

AAA authorization limits the services available to a user. When AAA authorization is enabled, the access point/bridge uses information retrieved from the user's profile, which is in the local user database or on the security server, to configure the user's session. The user is granted access to a requested service only if the information in the user profile allows it.



Note

This section describes setting up authorization for access point/bridge administrators, not for wireless client devices.

You can use the **aaa authorization** global configuration command with the **radius** keyword to set parameters that restrict a user's network access to privileged EXEC mode.

The **aaa authorization exec radius local** command sets these authorization parameters:

- Use RADIUS for privileged EXEC access authorization if authentication was performed by using RADIUS.
- Use the local database if authentication was not performed by using RADIUS.



Note

Authorization is bypassed for authenticated users who log in through the CLI even if authorization has been configured.

Beginning in privileged EXEC mode, follow these steps to specify RADIUS authorization for privileged EXEC access and network services:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	aaa authorization network radius	Configure the access point/bridge for user RADIUS authorization for all network-related service requests.
Step 3	aaa authorization exec radius	Configure the access point/bridge for user RADIUS authorization to determine if the user has privileged EXEC access. The exec keyword might return user profile information (such as autocommand information).
Step 4	end	Return to privileged EXEC mode.
Step 5	show running-config	Verify your entries.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To disable authorization, use the **no aaa authorization {network | exec} method1** global configuration command.

Starting RADIUS Accounting

The AAA accounting feature tracks the services that users are accessing and the amount of network resources that they are consuming. When AAA accounting is enabled, the access point/bridge reports user activity to the RADIUS security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server. This data can then be analyzed for network management, client billing, or auditing. See the [“RADIUS Attributes Sent by the Access Point/Bridge” section on page 12-18](#) for a complete list of attributes sent and honored by the access point/bridge.

Beginning in privileged EXEC mode, follow these steps to enable RADIUS accounting for each Cisco IOS privilege level and for network services:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	aaa accounting network start-stop radius	Enable RADIUS accounting for all network-related service requests.
Step 3	ip radius source-interface bvi1	Configure the access point/bridge to send its BVI IP address in the NAS_IP_ADDRESS attribute for accounting records.
Step 4	aaa accounting update periodic minutes	Enter an accounting update interval in minutes.
Step 5	end	Return to privileged EXEC mode.
Step 6	show running-config	Verify your entries.
Step 7	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To disable accounting, use the **no aaa accounting {network | exec} {start-stop} method1...** global configuration command.

Selecting the CSID Format

You can select the format for MAC addresses in Called-Station-ID (CSID) and Calling-Station-ID attributes in RADIUS packets. Use the **dot11 aaa csid** global configuration command to select the CSID format. Table 12-1 lists the format options with corresponding MAC address examples.

Table 12-1 CSID Format Options

Option	MAC Address Example
default	0007.85b3.5f4a
ietf	00-07-85-b3-5f-4a
unformatted	000785b35f4a

To return to the default CSID format, use the **no** form of the **dot11 aaa csid** command, or enter **dot11 aaa csid default**.



Note

You can also use the **wlccp wds aaa csid** command to select the CSID format.

Configuring Settings for All RADIUS Servers

Beginning in privileged EXEC mode, follow these steps to configure global communication settings between the access point/bridge and all RADIUS servers:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	radius-server key <i>string</i>	Specify the shared secret text string used between the access point/bridge and all RADIUS servers. Note The key is a text string that must match the encryption key used on the RADIUS server. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key.
Step 3	radius-server retransmit <i>retries</i>	Specify the number of times the access point/bridge sends each RADIUS request to the server before giving up. The default is 3; the range 1 to 1000.
Step 4	radius-server timeout <i>seconds</i>	Specify the number of seconds an access point/bridge waits for a reply to a RADIUS request before resending the request. The default is 5 seconds; the range is 1 to 1000.
Step 5	radius-server deadtime <i>minutes</i>	Use this command to cause the Cisco IOS software to mark as “dead” any RADIUS servers that fail to respond to authentication requests, thus avoiding the wait for the request to time out before trying the next configured server. A RADIUS server marked as dead is skipped by additional requests for the duration of minutes that you specify, up to a maximum of 1440 (24 hours). Note If you set up more than one RADIUS server, you must configure the RADIUS server deadtime for optimal performance.

	Command	Purpose
Step 6	radius-server attribute 32 include-in-access-req format %h	Configure the access point/bridge to send its system name in the NAS_ID attribute for authentication.
Step 7	end	Return to privileged EXEC mode.
Step 8	show running-config	Verify your settings.
Step 9	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To return to the default setting for retransmit, timeout, and deadtime, use the **no** forms of these commands.

Configuring the Access Point/Bridge to Use Vendor-Specific RADIUS Attributes

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific information between the access point/bridge and the RADIUS server by using the vendor-specific attribute (attribute 26). Vendor-specific attributes (VSAs) allow vendors to support their own extended attributes not suitable for general use. The Cisco RADIUS implementation supports one vendor-specific option by using the format recommended in the specification. Cisco's vendor ID is 9, and the supported option has vendor type 1, which is named *cisco-avpair*. The value is a string with this format:

```
protocol : attribute sep value *
```

Protocol is a value of the Cisco protocol attribute for a particular type of authorization. *Attribute* and *value* are an appropriate AV pair defined in the Cisco TACACS+ specification, and *sep* is = for mandatory attributes and the asterisk (*) for optional attributes. This allows the full set of features available for TACACS+ authorization to also be used for RADIUS.

For example, the following AV pair activates Cisco's *multiple named ip address pools* feature during IP authorization (during PPP's IPCP address assignment):

```
cisco-avpair= "ip:addr-pool=first"
```

The following example shows how to provide a user logging in from an access point/bridge with immediate access to privileged EXEC commands:

```
cisco-avpair= "shell:priv-lvl=15"
```

Other vendors have their own unique vendor IDs, options, and associated VSAs. For more information about vendor IDs and VSAs, refer to RFC 2138, "Remote Authentication Dial-In User Service (RADIUS)."

Beginning in privileged EXEC mode, follow these steps to configure the access point/bridge to recognize and use VSAs:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	radius-server vsa send [accounting authentication]	Enable the access point/bridge to recognize and use VSAs as defined by RADIUS IETF attribute 26. • (Optional) Use the accounting keyword to limit the set of recognized vendor-specific attributes to only accounting attributes. • (Optional) Use the authentication keyword to limit the set of recognized vendor-specific attributes to only authentication attributes. If you enter this command without keywords, both accounting and authentication vendor-specific attributes are used.
Step 3	end	Return to privileged EXEC mode.
Step 4	show running-config	Verify your settings.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

For a complete list of RADIUS attributes or more information about VSA 26, refer to the “RADIUS Attributes” appendix in the *Cisco IOS Security Configuration Guide for Release 12.2*.

Configuring the Access Point/Bridge for Vendor-Proprietary RADIUS Server Communication

Although an IETF draft standard for RADIUS specifies a method for communicating vendor-proprietary information between the access point/bridge and the RADIUS server, some vendors have extended the RADIUS attribute set in a unique way. Cisco IOS software supports a subset of vendor-proprietary RADIUS attributes.

As mentioned earlier, to configure RADIUS (whether vendor-proprietary or IETF draft-compliant), you must specify the host running the RADIUS server daemon and the secret text string it shares with the access point/bridge. You specify the RADIUS host and secret text string by using the **radius-server** global configuration commands.

Beginning in privileged EXEC mode, follow these steps to specify a vendor-proprietary RADIUS server host and a shared secret text string:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	radius-server host {hostname ip-address} non-standard	Specify the IP address or host name of the remote RADIUS server host and identify that it is using a vendor-proprietary implementation of RADIUS.

	Command	Purpose
Step 3	radius-server key <i>string</i>	Specify the shared secret text string used between the access point/bridge and the vendor-proprietary RADIUS server. The access point/bridge and the RADIUS server use this text string to encrypt passwords and exchange responses. Note The key is a text string that must match the encryption key used on the RADIUS server. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key.
Step 4	end	Return to privileged EXEC mode.
Step 5	show running-config	Verify your settings.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To delete the vendor-proprietary RADIUS host, use the **no radius-server host** *{hostname | ip-address}* **non-standard** global configuration command. To disable the key, use the **no radius-server key** global configuration command.

This example shows how to specify a vendor-proprietary RADIUS host and to use a secret key of *rad124* between the access point/bridge and the server:

```
AP(config)# radius-server host 172.20.30.15 nonstandard
AP(config)# radius-server key rad124
```

Configuring WISPr RADIUS Attributes

The Wi-Fi Alliance's *WISPr Best Current Practices for Wireless Internet Service Provider (WISP) Roaming* document lists RADIUS attributes that access point/bridges must send with RADIUS accounting and authentication requests. The access point/bridge currently supports only the WISPr location-name and the ISO and International Telecommunications Union (ITU) country and area codes attributes. Use the **snmp-server location** and the **dot11 location isocc** commands to configure these attributes on the access point/bridge.

The *WISPr Best Current Practices for Wireless Internet Service Provider (WISP) Roaming* document also requires the access point/bridge to include a class attribute in RADIUS authentication replies and accounting requests. The access point/bridge includes the class attribute automatically and does not have to be configured to do so.

You can find a list of ISO and ITU country and area codes at the ISO and ITU websites. Cisco IOS software does not check the validity of the country and area codes that you configure on the access point/bridge.

Beginning in privileged EXEC mode, follow these steps to specify WISPr RADIUS attributes on the access point/bridge:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	snmp-server location <i>location</i>	Specify the WISPr location-name attribute. The <i>WISPr Best Current Practices for Wireless Internet Service Provider (WISP) Roaming</i> document recommends that you enter the location name in this format: <i>hotspot_operator_name,location</i>
Step 3	dot11 location isocc <i>ISO-country-code</i> cc <i>country-code</i> ac <i>area-code</i>	Specify ISO and ITU country and area codes that the access point/bridge includes in accounting and authentication requests. • isocc <i>ISO-country-code</i>—specifies the ISO country code that the access point/bridge includes in RADIUS authentication and accounting requests • cc <i>country-code</i>—specifies the ITU country code that the access point/bridge includes in RADIUS authentication and accounting requests • ac <i>area-code</i>—specifies the ITU area code that the access point/bridge includes in RADIUS authentication and accounting requests
Step 4	end	Return to privileged EXEC mode.
Step 5	show running-config	Verify your settings.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to configure the WISPr location-name attribute:

```
ap# snmp-server location ACMEWISP,Gate_14_Terminal_C_of_Newark_Airport
```

This example shows how to configure the ISO and ITU location codes on the access point/bridge:

```
ap# dot11 location isocc us cc 1 ac 408
```

This example shows how the access point/bridge adds the SSID used by the client device and formats the location-ID string:

```
isocc=us,cc=1,ac=408,network=ACMEWISP_NewarkAirport
```

Displaying the RADIUS Configuration

To display the RADIUS configuration, use the **show running-config** privileged EXEC command.



Note

When DNS is configured on the access point/bridge, the **show running-config** command sometimes displays a server's IP address instead of its name.

RADIUS Attributes Sent by the Access Point/Bridge

Table 12-2 through Table 12-6 identify the attributes sent by an access point/bridge to a client in access-request, access-accept, and accounting-request packets.



Note

You can configure the access point/bridge to include in its RADIUS accounting and authentication requests attributes recommended by the Wi-Fi Alliance's *WISPr Best Current Practices for Wireless Internet Service Provider (WISP) Roaming* document. Refer to the [“Configuring WISPr RADIUS Attributes” section on page 12-16](#) for instructions.

Table 12-2 **Attributes Sent in Access-Request Packets**

Attribute ID	Description
1	User-Name
4	NAS-IP-Address
5	NAS-Port
12	Framed-MTU
30	Called-Station-ID (MAC address)
31	Calling-Station-ID (MAC address)
32	NAS-Identifier ¹
61	NAS-Port-Type
79	EAP-Message
80	Message-Authenticator

1. The access point/bridge sends the NAS-Identifier if attribute 32 (include-in-access-req) is configured.

Table 12-3 **Attributes Honored in Access-Accept Packets**

Attribute ID	Description
25	Class
27	Session-Timeout
64	Tunnel-Type ¹
65	Tunnel-Medium-Type ¹
79	EAP-Message
80	Message-Authenticator
81	Tunnel-Private-Group-ID ¹
VSA (attribute 26)	LEAP session-key
VSA (attribute 26)	Auth-Algo-Type
VSA (attribute 26)	SSID

1. RFC2868; defines a VLAN override number.

Table 12-4 *Attributes Sent in Accounting-Request (start) Packets*

Attribute ID	Description
1	User-Name
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
25	Class
41	Acct-Delay-Time
44	Acct-Session-Id
61	NAS-Port-Type
VSA (attribute 26)	SSID
VSA (attribute 26)	NAS-Location
VSA (attribute 26)	Cisco-NAS-Port
VSA (attribute 26)	Interface

Table 12-5 *Attributes Sent in Accounting-Request (update) Packets*

Attribute ID	Description
1	User-Name
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
25	Class
41	Acct-Delay-Time
42	Acct-Input-Octets
43	Acct-Output-Octets
44	Acct-Session-Id
46	Acct-Session-Time
47	Acct-Input-Packets
48	Acct-Output-Packets
61	NAS-Port-Type
VSA (attribute 26)	SSID
VSA (attribute 26)	NAS-Location
VSA (attribute 26)	VLAN-ID
VSA (attribute 26)	Connect-Progress
VSA (attribute 26)	Cisco-NAS-Port
VSA (attribute 26)	Interface

Table 12-6 *Attributes Sent in Accounting-Request (stop) Packets*

Attribute ID	Description
1	User-Name
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
25	Class
41	Acct-Delay-Time
42	Acct-Input-Octets
43	Acct-Output-Octets
44	Acct-Session-Id
46	Acct-Session-Time
47	Acct-Input-Packets
48	Acct-Output-Packets
49	Acct-Terminate-Cause
61	NAS-Port-Type
VSA (attribute 26)	SSID
VSA (attribute 26)	NAS-Location
VSA (attribute 26)	Disc-Cause-Ext
VSA (attribute 26)	VLAN-ID
VSA (attribute 26)	Connect-Progress
VSA (attribute 26)	Cisco-NAS-Port
VSA (attribute 26)	Interface
VSA (attribute 26)	Auth-Algo-Type

**Note**

By default, the access point/bridge sends reauthentication requests to the authentication server with the service-type attribute set to authenticate-only. However, some Microsoft IAS servers do not support the authenticate-only service-type attribute. Changing the service-type attribute to login-only ensures that Microsoft IAS servers recognize reauthentication requests from the access point/bridge. Use the **dot11 aaa authentication attributes service-type login-only** global configuration command to set the service-type attribute in reauthentication requests to login-only.

Configuring and Enabling TACACS+

This section contains this configuration information:

- [Understanding TACACS+, page 12-21](#)
- [TACACS+ Operation, page 12-22](#)
- [Configuring TACACS+, page 12-22](#)
- [Displaying the TACACS+ Configuration, page 12-27](#)

Understanding TACACS+

TACACS+ is a security application that provides centralized validation of users attempting to gain access to your access point/bridge. Unlike RADIUS, TACACS+ does not authenticate client devices associated to the access point/bridge.

TACACS+ services are maintained in a database on a TACACS+ daemon typically running on a UNIX or Windows NT workstation. You should have access to and should configure a TACACS+ server before configuring TACACS+ features on your access point/bridge.

TACACS+ provides for separate and modular authentication, authorization, and accounting facilities. TACACS+ allows for a single access control server (the TACACS+ daemon) to provide each service—authentication, authorization, and accounting—independently. Each service can be tied into its own database to take advantage of other services available on that server or on the network, depending on the capabilities of the daemon.

TACACS+, administered through the AAA security services, can provide these services:

- **Authentication**—Provides complete control of authentication of administrators through login and password dialog, challenge and response, and messaging support.
The authentication facility can conduct a dialog with the administrator (for example, after a username and password are provided, to challenge a user with several questions, such as home address, mother's maiden name, service type, and social security number). The TACACS+ authentication service can also send messages to administrator screens. For example, a message could notify administrators that their passwords must be changed because of the company's password aging policy.
- **Authorization**—Provides fine-grained control over administrator capabilities for the duration of the administrator's session, including but not limited to setting autocommands, access control, session duration, or protocol support. You can also enforce restrictions on the commands that an administrator can execute with the TACACS+ authorization feature.
- **Accounting**—Collects and sends information used for billing, auditing, and reporting to the TACACS+ daemon. Network managers can use the accounting facility to track administrator activity for a security audit or to provide information for user billing. Accounting records include administrator identities, start and stop times, executed commands (such as PPP), number of packets, and number of bytes.

The TACACS+ protocol provides authentication between the access point/bridge and the TACACS+ daemon, and it ensures confidentiality because all protocol exchanges between the access point/bridge and the TACACS+ daemon are encrypted.

You need a system running the TACACS+ daemon software to use TACACS+ on your access point/bridge.

TACACS+ Operation

When an administrator attempts a simple ASCII login by authenticating to an access point/bridge using TACACS+, this process occurs:

1. When the connection is established, the access point/bridge contacts the TACACS+ daemon to obtain a username prompt, which is then displayed to the administrator. The administrator enters a username, and the access point/bridge then contacts the TACACS+ daemon to obtain a password prompt. The access point/bridge displays the password prompt to the administrator, the administrator enters a password, and the password is then sent to the TACACS+ daemon.

TACACS+ allows a conversation to be held between the daemon and the administrator until the daemon receives enough information to authenticate the administrator. The daemon prompts for a username and password combination, but can include other items, such as the user's mother's maiden name.

2. The access point/bridge eventually receives one of these responses from the TACACS+ daemon:
 - ACCEPT—The administrator is authenticated and service can begin. If the access point/bridge is configured to require authorization, authorization begins at this time.
 - REJECT—The administrator is not authenticated. The administrator can be denied access or is prompted to retry the login sequence, depending on the TACACS+ daemon.
 - ERROR—An error occurred at some time during authentication with the daemon or in the network connection between the daemon and the access point/bridge. If an ERROR response is received, the access point/bridge typically tries to use an alternative method for authenticating the administrator.
 - CONTINUE—The administrator is prompted for additional authentication information.

After authentication, the administrator undergoes an additional authorization phase if authorization has been enabled on the access point/bridge. Administrators must first successfully complete TACACS+ authentication before proceeding to TACACS+ authorization.

3. If TACACS+ authorization is required, the TACACS+ daemon is again contacted, and it returns an ACCEPT or REJECT authorization response. If an ACCEPT response is returned, the response contains data in the form of attributes that direct the EXEC or NETWORK session for that administrator, determining the services that the administrator can access:
 - Telnet, rlogin, or privileged EXEC services
 - Connection parameters, including the host or client IP address, access list, and administrator timeouts

Configuring TACACS+

This section describes how to configure your access point/bridge to support TACACS+. At a minimum, you must identify the host or hosts maintaining the TACACS+ daemon and define the method lists for TACACS+ authentication. You can optionally define method lists for TACACS+ authorization and accounting. A method list defines the sequence and methods to be used to authenticate, to authorize, or to keep accounts on an administrator. You can use method lists to designate one or more security protocols to be used, thus ensuring a backup system if the initial method fails. The software uses the first method listed to authenticate, to authorize, or to keep accounts on administrators; if that method does not respond, the software selects the next method in the list. This process continues until there is successful communication with a listed method or the method list is exhausted.

This section contains this configuration information:

- [Default TACACS+ Configuration, page 12-23](#)
- [Identifying the TACACS+ Server Host and Setting the Authentication Key, page 12-23](#)
- [Configuring TACACS+ Login Authentication, page 12-24](#)
- [Configuring TACACS+ Authorization for Privileged EXEC Access and Network Services, page 12-25](#)
- [Starting TACACS+ Accounting, page 12-26](#)

Default TACACS+ Configuration

TACACS+ and AAA are disabled by default.

To prevent a lapse in security, you cannot configure TACACS+ through a network management application. When enabled, TACACS+ can authenticate administrators accessing the access point/bridge through the CLI.

Identifying the TACACS+ Server Host and Setting the Authentication Key

You can configure the access point/bridge to use a single server or AAA server groups to group existing server hosts for authentication. You can group servers to select a subset of the configured server hosts and use them for a particular service. The server group is used with a global server-host list and contains the list of IP addresses of the selected server hosts.

Beginning in privileged EXEC mode, follow these steps to identify the IP host or host maintaining TACACS+ server and optionally set the encryption key:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	tacacs-server host <i>hostname</i> [port <i>integer</i>] [timeout <i>integer</i>] [key <i>string</i>]	Identify the IP host or hosts maintaining a TACACS+ server. Enter this command multiple times to create a list of preferred hosts. The software searches for hosts in the order in which you specify them. • For <i>hostname</i>, specify the name or IP address of the host. • (Optional) For port <i>integer</i>, specify a server port number. The default is port 49. The range is 1 to 65535. • (Optional) For timeout <i>integer</i>, specify a time in seconds the access point/bridge waits for a response from the daemon before it times out and declares an error. The default is 5 seconds. The range is 1 to 1000 seconds. • (Optional) For key <i>string</i>, specify the encryption key for encrypting and decrypting all traffic between the access point/bridge and the TACACS+ daemon. You must configure the same key on the TACACS+ daemon for encryption to be successful.
Step 3	aaa new-model	Enable AAA.
Step 4	aaa group server tacacs+ <i>group-name</i>	(Optional) Define the AAA server-group with a group name. This command puts the access point/bridge in a server group subconfiguration mode.

	Command	Purpose
Step 5	server <i>ip-address</i>	(Optional) Associate a particular TACACS+ server with the defined server group. Repeat this step for each TACACS+ server in the AAA server group. Each server in the group must be previously defined in Step 2.
Step 6	end	Return to privileged EXEC mode.
Step 7	show tacacs	Verify your entries.
Step 8	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To remove the specified TACACS+ server name or address, use the **no tacacs-server host** *hostname* global configuration command. To remove a server group from the configuration list, use the **no aaa group server tacacs+ group-name** global configuration command. To remove the IP address of a TACACS+ server, use the **no server ip-address** server group subconfiguration command.

Configuring TACACS+ Login Authentication

To configure AAA authentication, you define a named list of authentication methods and then apply that list to various interfaces. The method list defines the types of authentication to be performed and the sequence in which they are performed; it must be applied to a specific interface before any of the defined authentication methods are performed. The only exception is the default method list (which, by coincidence, is named *default*). The default method list is automatically applied to all interfaces except those that have a named method list explicitly defined. A defined method list overrides the default method list.

A method list describes the sequence and authentication methods to be queried to authenticate an administrator. You can designate one or more security protocols to be used for authentication, thus ensuring a backup system for authentication in case the initial method fails. The software uses the first method listed to authenticate users; if that method fails to respond, the software selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this cycle—meaning that the security server or local username database responds by denying the administrator access—the authentication process stops, and no other authentication methods are attempted.

Beginning in privileged EXEC mode, follow these steps to configure login authentication:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	aaa new-model	Enable AAA.

	Command	Purpose
Step 3	aaa authentication login { default <i>list-name</i> } <i>method1</i> [<i>method2</i> ...]	Create a login authentication method list. - To create a default list that is used when a named list is <i>not</i> specified in the login authentication command, use the default keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all interfaces. - For <i>list-name</i>, specify a character string to name the list you are creating. - For <i>method1</i>..., specify the actual method the authentication algorithm tries. The additional methods of authentication are used only if the previous method returns an error, not if it fails. Select one of these methods: line—Use the line password for authentication. You must define a line password before you can use this authentication method. Use the password <i>password</i> line configuration command. local—Use the local username database for authentication. You must enter username information into the database. Use the username <i>password</i> global configuration command. tacacs+—Uses TACACS+ authentication. You must configure the TACACS+ server before you can use this authentication method.
Step 4	line [console tty vtty] <i>line-number</i> [<i>ending-line-number</i>]	Enter line configuration mode, and configure the lines to which you want to apply the authentication list.
Step 5	login authentication { default <i>list-name</i> }	Apply the authentication list to a line or set of lines. - If you specify default, use the default list created with the aaa authentication login command. - For <i>list-name</i>, specify the list created with the aaa authentication login command.
Step 6	end	Return to privileged EXEC mode.
Step 7	show running-config	Verify your entries.
Step 8	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To disable AAA, use the **no aaa new-model** global configuration command. To disable AAA authentication, use the **no aaa authentication login** { **default** | *list-name* } *method1* [*method2*...] global configuration command. To either disable TACACS+ authentication for logins or to return to the default value, use the **no login authentication** { **default** | *list-name* } line configuration command.

Configuring TACACS+ Authorization for Privileged EXEC Access and Network Services

AAA authorization limits the services available to an administrator. When AAA authorization is enabled, the access point/bridge uses information retrieved from the administrator's profile, which is located either in the local user database or on the security server, to configure the administrator's session. The administrator is granted access to a requested service only if the information in the administrator profile allows it.

You can use the **aaa authorization** global configuration command with the **tacacs+** keyword to set parameters that restrict an administrator's network access to privileged EXEC mode.

The **aaa authorization exec tacacs+ local** command sets these authorization parameters:

- Use TACACS+ for privileged EXEC access authorization if authentication was performed by using TACACS+.
- Use the local database if authentication was not performed by using TACACS+.


Note

Authorization is bypassed for authenticated administrators who log in through the CLI even if authorization has been configured.

Beginning in privileged EXEC mode, follow these steps to specify TACACS+ authorization for privileged EXEC access and network services:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	aaa authorization network tacacs+	Configure the access point/bridge for administrator TACACS+ authorization for all network-related service requests.
Step 3	aaa authorization exec tacacs+	Configure the access point/bridge for administrator TACACS+ authorization to determine if the administrator has privileged EXEC access. The exec keyword might return user profile information (such as autocommand information).
Step 4	end	Return to privileged EXEC mode.
Step 5	show running-config	Verify your entries.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To disable authorization, use the **no aaa authorization {network | exec} method1** global configuration command.

Starting TACACS+ Accounting

The AAA accounting feature tracks the services that administrators are accessing and the amount of network resources that they are consuming. When AAA accounting is enabled, the access point/bridge reports administrator activity to the TACACS+ security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server. This data can then be analyzed for network management, client billing, or auditing.

Beginning in privileged EXEC mode, follow these steps to enable TACACS+ accounting for each Cisco IOS privilege level and for network services:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	aaa accounting network start-stop tacacs+	Enable TACACS+ accounting for all network-related service requests.
Step 3	aaa accounting exec start-stop tacacs+	Enable TACACS+ accounting to send a start-record accounting notice at the beginning of a privileged EXEC process and a stop-record at the end.
Step 4	end	Return to privileged EXEC mode.

	Command	Purpose
Step 5	show running-config	Verify your entries.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To disable accounting, use the **no aaa accounting {network | exec} {start-stop} method1...** global configuration command.

Displaying the TACACS+ Configuration

To display TACACS+ server statistics, use the **show tacacs** privileged EXEC command.



Configuring VLANs

This chapter describes how to configure your access point/bridge to operate with the VLANs set up on your wired LAN. These sections describe how to configure your access point/bridge to support VLANs:

- [Understanding VLANs, page 13-2](#)
- [Configuring VLANs, page 13-4](#)

Understanding VLANs

A VLAN is a switched network that is logically segmented, by functions, project teams, or applications rather than on a physical or geographical basis. For example, all workstations and servers used by a particular workgroup team can be connected to the same VLAN, regardless of their physical connections to the network or the fact that they might be intermingled with other teams. You use VLANs to reconfigure the network through software rather than physically unplugging and moving devices or wires.

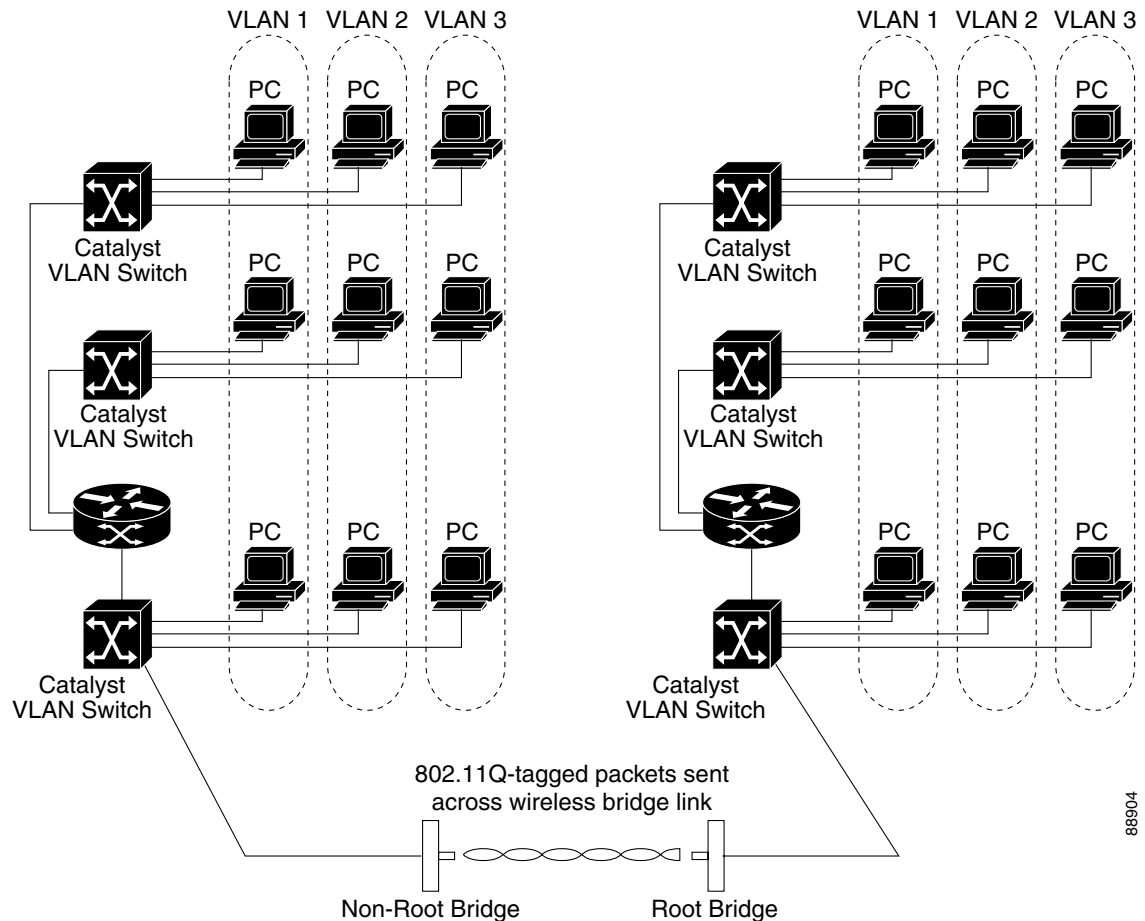
A VLAN can be thought of as a broadcast domain that exists within a defined set of switches. A VLAN consists of a number of end systems, either hosts or network equipment (such as access point/bridges and routers), connected by a single bridging domain. The bridging domain is supported on various pieces of network equipment such as LAN switches that operate bridging protocols between them with a separate group for each VLAN.

VLANs provide the segmentation services traditionally provided by routers in LAN configurations. VLANs address scalability, security, and network management. You should consider several key issues when designing and building switched LAN networks:

- LAN segmentation
- Security
- Broadcast control
- Performance
- Network management
- Communication between VLANs

You extend VLANs into a wireless LAN by adding IEEE 802.11Q tag awareness to the access point/bridge. Frames destined for different VLANs are transmitted by the access point/bridge wirelessly on different SSIDs with different WEP keys. Only the clients associated with that VLAN receive those packets. Conversely, packets coming from a client associated with a certain VLAN are 802.11Q tagged before they are forwarded onto the wired network.

[Figure 13-1](#) shows two access point/bridges sending 802.11Q-tagged packets between two LAN segments that use logical VLAN segmentation.

Figure 13-1 AN and VLAN Segmentation with Wireless Devices

Related Documents

These documents provide more detailed information pertaining to VLAN design and configuration:

- *Cisco IOS Switching Services Configuration Guide*. Click this link to browse to this document: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fswtch_c/index.htm
- *Cisco Internetwork Design Guide*. Click this link to browse to this document: <http://www.cisco.com/univercd/cc/td/doc/cisintwk/idg4/index.htm>
- *Cisco Internetworking Technology Handbook*. Click this link to browse to this document: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/index.htm
- *Cisco Internetworking Troubleshooting Guide*. Click this link to browse to this document: http://www.cisco.com/univercd/cc/td/doc/cisintwk/itg_v1/index.htm

Incorporating Wireless Access Point/Bridges into VLANs

The basic wireless components of a VLAN consist of an access point and a client associated to it using wireless technology. The access point is physically connected through a trunk port to the network VLAN switch on which the VLAN is configured. The physical connection to the VLAN switch is through the access point's Ethernet port.

In fundamental terms, the key to configuring an access point/bridge to connect to a specific VLAN is to configure its SSID to recognize that VLAN. Because VLANs are identified by a VLAN ID or name, it follows that if the SSID on an access point/bridge is configured to recognize a specific VLAN ID or name, a connection to the VLAN is established. When this connection is made, associated wireless client devices having the same SSID can access the VLAN through the access point/bridge. The VLAN processes data to and from the clients the same way that it processes data to and from wired connections. You can configure up to 16 SSIDs on your access point/bridge, so you can support up to 16 VLANs. You can assign only one SSID to a VLAN.

You can use the VLAN feature to deploy wireless devices with greater efficiency and flexibility. For example, one access point/bridge can now handle the specific requirements of multiple users having widely varied network access and permissions. Without VLAN capability, multiple access point/bridges would have to be employed to serve classes of users based on the access and permissions they were assigned.

These are two common strategies for deploying wireless VLANs:

- **Segmentation by user groups:** You can segment your wireless LAN user community and enforce a different security policy for each user group. For example, you can create three wired and wireless VLANs in an enterprise environment for full-time and part-time employees and also provide guest access.
- **Segmentation by device types:** You can segment your wireless LAN to allow different devices with different security capabilities to join the network. For example, some wireless users might have handheld devices that support only static WEP, and some wireless users might have more sophisticated devices using dynamic WEP. You can group and isolate these devices into separate VLANs.

**Note**

You cannot configure multiple VLANs on an access point/bridge configured as a repeater access point. Repeater access points support only the native VLAN.

Configuring VLANs

These sections describe how to configure VLANs on your access point/bridge:

- [Configuring a VLAN, page 13-4](#)
- [Viewing VLANs Configured on the Access Point/Bridge, page 13-7](#)

Configuring a VLAN

Configuring your access point/bridge to support VLANs is a five-step process:

1. Create subinterfaces on the radio and Ethernet interfaces.
2. Enable 802.1q encapsulation on the subinterfaces and assign one subinterface as the native VLAN.

3. Assign an access point/bridge group to each VLAN.
4. (Optional) Enable WEP on the native VLAN.
5. Assign the access point/bridge's SSID to the native VLAN.

This section describes how to assign an SSID to a VLAN and how to enable a VLAN on the access point/bridge radio and Ethernet ports. For detailed instructions on assigning authentication types to SSIDs, see [Chapter 10, “Configuring Authentication Types.”](#)

Beginning in privileged EXEC mode, follow these steps to assign an SSID to a VLAN and enable the VLAN on the access point/bridge radio and Ethernet ports:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio0.x	Create a radio subinterface and enter interface configuration mode for the subinterface.
Step 3	encapsulation dot1q <i>vlan-id</i> [native]	Enable a VLAN on the subinterface. (Optional) Designate the VLAN as the native VLAN. On many networks, the native VLAN is VLAN 1.
Step 4	bridge-group <i>number</i>	Assign the subinterface to a bridge group. You can number your bridge groups from 1 to 255. Note When you enter the bridge-group command, the bridge enables the subinterface to be ready to participate in STP when you enter the bridge <i>n</i> protocol ieee command. See Chapter 8, “Configuring Spanning Tree Protocol,” for complete instructions on enabling STP on the bridge.
Step 5	exit	Return to global configuration mode.
Step 6	interface fastEthernet0.x	Create an Ethernet subinterface and enter interface configuration mode for the subinterface.
Step 7	encapsulation dot1q <i>vlan-id</i> [native]	Enable a VLAN on the subinterface. (Optional) Designate the VLAN as the native VLAN. On many networks, the native VLAN is VLAN 1.
Step 8	bridge-group <i>number</i>	Assign the subinterface to a bridge group. You can number your bridge groups from 1 to 255.
Step 9	exit	Return to global configuration mode.
Step 10	interface dot11radio 0	Enter interface configuration mode for the radio interface.
Step 11	ssid <i>ssid-string</i>	Create an SSID and enter SSID configuration mode for the new SSID. The SSID can consist of up to 32 alphanumeric characters. SSIDs are case sensitive. You can create only one SSID on the access point/bridge. Note You use the ssid command's authentication options to configure an authentication type for each SSID. See Chapter 10, “Configuring Authentication Types,” for instructions on configuring authentication types.
Step 12	vlan <i>vlan-id</i>	Assign the SSID to the native VLAN.

	Command	Purpose
Step 13	infrastructure-ssid	Designate the SSID as the infrastructure SSID. It is used to instruct a non-root access point/bridge or workgroup bridge radio to associate with this SSID.
Step 14	encryption [vlan <i>vlan-id</i>] mode wep { optional [key-hash] mandatory [mic] [key-hash]}	(Optional) Enable WEP and WEP features on the native VLAN. (Optional) Select the VLAN for which you want to enable WEP and WEP features. - Set the WEP level and enable TKIP and MIC. If you enter optional, another access point/bridge can associate to the access point/bridge with or without WEP enabled. You can enable TKIP with WEP set to optional but you cannot enable MIC. If you enter mandatory, other access point/bridges must have WEP enabled to associate to the access point/bridge. You can enable both TKIP and MIC with WEP set to mandatory. Note You can enable encryption for each VLAN, but the access point/bridge uses only the encryption on the native VLAN. For example, if the native VLAN encryption is set to 128-bit static WEP, that is the only encryption method used for traffic between the root and non-root access point/bridge.
Step 15	exit	Return to interface configuration mode for the radio interface.
Step 16	end	Return to privileged EXEC mode.
Step 17	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to:

- Enable the VLAN on the radio and Ethernet ports as the native VLAN
- Name an SSID
- Assign the SSID to a VLAN

```

ap# configure terminal
ap(config)# interface dot11radio0.1
ap(config-subif)# encapsulation dot1q 1 native
ap(config-subif)# bridge group 1
ap(config-subif)# exit
ap(config)# interface fastEthernet0.1
ap(config-subif)# encapsulation dot1q 1 native
ap(config-subif)# bridge group 1
ap(config-subif)# exit
ap(config)# interface dot11radio0
ap(config-if)# ssid batman
ap(config-ssid)# vlan 1
ap(config-ssid)# infrastructure-ssid
ap(config-ssid)# end

```

Viewing VLANs Configured on the Access Point/Bridge

In privileged EXEC mode, use the **show vlan** command to view the VLANs that the access point/bridge supports. This is sample output from a **show vlan** command:

```
Virtual LAN ID: 1 (IEEE 802.1Q Encapsulation)

    vLAN Trunk Interfaces: Dot11Radio0
FastEthernet0
Virtual-Dot11Radio0

    This is configured as native Vlan for the following interface(s) :
Dot11Radio0
FastEthernet0
Virtual-Dot11Radio0

    Protocols Configured:   Address:           Received:         Transmitted:
        Bridging           Bridge Group 1      201688            0
        Bridging           Bridge Group 1      201688            0
        Bridging           Bridge Group 1      201688            0

Virtual LAN ID: 2 (IEEE 802.1Q Encapsulation)

    vLAN Trunk Interfaces: Dot11Radio0.2
FastEthernet0.2
Virtual-Dot11Radio0.2

    Protocols Configured:   Address:           Received:         Transmitted:
```

Assigning Names to VLANs

You can assign a name to a VLAN in addition to its numerical ID. VLAN names can contain up to 32 ASCII characters. The access point/bridge stores each VLAN name and ID pair in a table.

Guidelines for Using VLAN Names

Keep these guidelines in mind when using VLAN names:

- The mapping of a VLAN name to a VLAN ID is local to each access point/bridge, so across your network, you can assign the same VLAN name to a different VLAN ID.



Note

If clients on your wireless LAN require seamless roaming, Cisco recommends that you assign the same VLAN name to the same VLAN ID across all access point/bridges, or that you use only VLAN IDs without names.

- Every VLAN configured on your access point/bridge must have an ID, but VLAN names are optional.
- VLAN names can contain up to 32 ASCII characters. However, a VLAN name cannot be a number between 1 and 4095. For example, *vlan4095* is a valid VLAN name, but *4095* is not. The access point/bridge reserves the numbers 1 through 4095 for VLAN IDs.

Creating a VLAN Name

Beginning in privileged EXEC mode, follow these steps to assign a name to a VLAN:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	dot11 vlan-name <i>name</i> vlan <i>vlan-id</i>	Assign a VLAN name to a VLAN ID. The name can contain up to 32 ASCII characters.
Step 3	end	Return to privileged EXEC mode.
Step 4	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Use the **no** form of the command to remove the name from the VLAN. Use the **show dot11 vlan-name** privileged EXEC command to list all the VLAN name and ID pairs configured on the access point/bridge.

Using a RADIUS Server to Assign Users to VLANs

You can configure your RADIUS authentication server to assign users or groups of users to a specific VLAN when they authenticate to the network.



Note

Unicast and multicast cipher suites advertised in WPA information element (and negotiated during 802.11 association) may potentially mismatch with the cipher suite supported in an explicitly assigned VLAN. If the RADIUS server assigns a new vlan ID which uses a different cipher suite from the previously negotiated cipher suite, there is no way for the access point/bridge and client to switch back to the new cipher suite. Currently, the WPA and CCKM protocols do not allow the cipher suite to be changed after the initial 802.11 cipher negotiation phase. In this scenario, the client device is disassociated from the wireless LAN.

The VLAN-mapping process consists of these steps:

1. A client device associates to the access point/bridge using any SSID configured on the access point/bridge.
2. The client begins RADIUS authentication.
3. When the client authenticates successfully, the RADIUS server maps the client to a specific VLAN, regardless of the VLAN mapping defined for the SSID the client is using on the access point/bridge. If the server does not return any VLAN attribute for the client, the client is assigned to the VLAN specified by the SSID mapped locally on the access point/bridge.

These are the RADIUS user attributes used for vlan-id assignment. Each attribute must have a common tag value between 1 and 31 to identify the grouped relationship.

- IETF 64 (Tunnel Type): Set this attribute to **VLAN**
- IETF 65 (Tunnel Medium Type): Set this attribute to **802**
- IETF 81 (Tunnel Private Group ID): Set this attribute to *vlan-id*

Viewing VLANs Configured on the Access Point/Bridge

In privileged EXEC mode, use the **show vlan** command to view the VLANs that the access point/bridge supports. This is sample output from a **show vlan** command:

```
Virtual LAN ID: 1 (IEEE 802.1Q Encapsulation)

    vLAN Trunk Interfaces: Dot11Radio0
FastEthernet0
Virtual-Dot11Radio0

    This is configured as native Vlan for the following interface(s) :
Dot11Radio0
FastEthernet0
Virtual-Dot11Radio0

    Protocols Configured:  Address:                Received:      Transmitted:
        Bridging          Bridge Group 1      201688         0
        Bridging          Bridge Group 1      201688         0
        Bridging          Bridge Group 1      201688         0

Virtual LAN ID: 2 (IEEE 802.1Q Encapsulation)

    vLAN Trunk Interfaces: Dot11Radio0.2
FastEthernet0.2
Virtual-Dot11Radio0.2

    Protocols Configured:  Address:                Received:      Transmitted:
```

VLAN Configuration Example

This example shows how to use VLANs to manage wireless devices on a college campus. In this example, three levels of access are available through VLANs configured on the wired network:

- **Management access**—Highest level of access; users can access all internal drives and files, departmental databases, top-level financial information, and other sensitive information. Management users are required to authenticate using Cisco LEAP.
- **Faculty access**—Medium level of access; users can access school's Intranet and Internet, access internal files, access student databases, and view internal information such as human resources, payroll, and other faculty-related material. Faculty users are required to authenticate using Cisco LEAP.
- **Student access**—Lowest level of access; users can access school's Intranet and the Internet, obtain class schedules, view grades, make appointments, and perform other student-related activities. Students are allowed to join the network using static WEP.

In this scenario, a minimum of three VLAN connections are required, one for each level of access. Because the access point/bridge can handle up to 16 SSIDs, you can use the basic design shown in [Table 13-1](#).

Table 13-1 Access Level SSID and VLAN Assignment

Level of Access	SSID	VLAN ID
Management	boss	01
Faculty	teach	02
Student	learn	03

Managers configure their wireless client adapters to use SSID boss, faculty members configure their clients to use SSID teach, and students configure their wireless client adapters to use SSID learn. When these clients associate to the access point/bridge, they automatically belong to the correct VLAN.

You would complete these steps to support the VLANs in this example:

1. Configure or confirm the configuration of these VLANs on one of the switches on your LAN.
2. On the access point/bridge, assign an SSID to each VLAN.
3. Assign authentication types to each SSID.
4. Configure VLAN 1, the Management VLAN, on both the fastethernet and dot11radio interfaces on the access point/bridge. You should make this VLAN the native VLAN.
5. Configure VLANs 2 and 3 on both the fastethernet and dot11radio interfaces on the access point/bridge.
6. Configure the client devices.

Table 13-2 shows the commands needed to configure the three VLANs in this example.

Table 13-2 Configuration Commands for VLAN Example

Configuring VLAN 1	Configuring VLAN 2	Configuring VLAN 3
<pre>br1300Router# configure terminal br1300Router(config)# interface dot11radio 0/0 br1300Router(config-if)# ssid boss br1300Router(config-ssid)# vlan 01 br1300Router(config-ssid)# end</pre>	<pre>br1300Router# configure terminal br1300Router(config)# interface dot11radio 0/0 br1300Router(config-if)# ssid teach br1300Router(config-ssid)# vlan 02 br1300Router(config-ssid)# end</pre>	<pre>br1300Router# configure terminal br1300Routerbr1300Router(config)# interface dot11radio 0/0 br1300Router(config-if)# ssid learn br1300Router(config-ssid)# vlan 03 br1300Router(config-ssid)# end</pre>

Table 13-2 Configuration Commands for VLAN Example (continued)

Configuring VLAN 1	Configuring VLAN 2	Configuring VLAN 3
<pre>br1300Router configure terminal br1300Router(config) interface FastEthernet0.1 br1300Router(config-subif) encapsulation dot1Q 1 native br1300Router(config-subif) exit</pre>	<pre>br1300Router(config) interface FastEthernet0.2 br1300Router(config-subif) encapsulation dot1Q 2 br1300Router(config-subif) bridge-group 2 br1300Router(config-subif) exit</pre>	<pre>br1300Router(config) interface FastEthernet0.3 br1300Router(config-subif) encapsulation dot1Q 3 br1300Router(config-subif) bridge-group 3 br1300Router(config-subif) exit</pre>
<pre>br1300Router(config)# interface Dot11Radio 0/0.1 br1300Router(config-subif)# encapsulation dot1Q 1 native br1300Router(config-subif)# exit</pre> Note You do not need to configure a bridge group on the subinterface that you set up as the native VLAN. This bridge group is moved to the native subinterface automatically to maintain the link to BVI 1, which represents both the radio and Ethernet interfaces.	<pre>br1300Router(config) interface Dot11Radio 0/0.2 br1300Router(config-subif) encapsulation dot1Q 2 br1300Router(config-subif) bridge-group 2 br1300Router(config-subif) exit</pre>	<pre>br1300Router(config) interface Dot11Radio 0/0.3 br1300Router(config-subif) encapsulation dot1Q 3 br1300Router(config-subif) bridge-group 3 br1300Router(config-subif) exit</pre>

Table 13-3 shows the results of the configuration commands in Table 13-2. Use the **show running** command to display the running configuration on the access point/bridge.

Table 13-3 Results of Example Configuration Commands

VLAN 1 Interfaces	VLAN 2 Interfaces	VLAN 3 Interfaces
<pre>interface Dot11Radio0/0.1 encapsulation dot1Q 1 native no ip route-cache no cdp enable bridge-group 1 bridge-group 1 subscriber-loop-control bridge-group 1 block-unknown-source no bridge-group 1 source-learning no bridge-group 1 unicast-flooding bridge-group 1 spanning-disabled</pre>	<pre>interface Dot11Radio0/0.2 encapsulation dot1Q 2 no ip route-cache no cdp enable bridge-group 2 bridge-group 2 subscriber-loop-control bridge-group 2 block-unknown-source no bridge-group 2 source-learning no bridge-group 2 unicast-flooding bridge-group 2 spanning-disabled</pre>	<pre>interface Dot11Radio0/0.3 encapsulation dot1Q 3 no ip route-cache bridge-group 3 bridge-group 3 subscriber-loop-control bridge-group 3 block-unknown-source no bridge-group 3 source-learning no bridge-group 3 unicast-flooding bridge-group 3 spanning-disabled</pre>
<pre>interface FastEthernet0.1 encapsulation dot1Q 1 native no ip route-cache bridge-group 1 no bridge-group 1 source-learning bridge-group 1 spanning-disabled</pre>	<pre>interface FastEthernet0.2 encapsulation dot1Q 2 no ip route-cache bridge-group 2 no bridge-group 2 source-learning bridge-group 2 spanning-disabled</pre>	<pre>interface FastEthernet0.3 encapsulation dot1Q 3 no ip route-cache bridge-group 3 no bridge-group 3 source-learning bridge-group 3 spanning-disabled</pre>

Notice that when you configure a bridge group on the radio interface, these commands are set automatically:

```
bridge-group 2 subscriber-loop-control  
bridge-group 2 block-unknown-source  
no bridge-group 2 source-learning  
no bridge-group 2 unicast-flooding  
bridge-group 2 spanning-disabled
```

When you configure a bridge group on the FastEthernet interface, these commands are set automatically:

```
no bridge-group 2 source-learning  
bridge-group 2 spanning-disabled
```



Configuring QoS

This chapter describes how to configure quality of service (QoS) on your access point/bridge. With this feature, you can provide preferential treatment to certain traffic at the expense of others. Without QoS, the access point/bridge offers best-effort service to each packet, regardless of the packet contents or size. It sends the packets without any assurance of reliability, delay bounds, or throughput.



Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges* for this release.

This chapter consists of these sections:

- [Understanding QoS for Wireless LANs, page 14-2](#)
- [Configuring QoS, page 14-5](#)
- [QoS Configuration Examples, page 14-12](#)

Understanding QoS for Wireless LANs

Typically, networks operate on a best-effort delivery basis, which means that all traffic has equal priority and an equal chance of being delivered in a timely manner. When congestion occurs, all traffic has an equal chance of being dropped.

When you configure QoS on the access point/bridge, you can select specific network traffic, prioritize it, and use congestion-management and congestion-avoidance techniques to provide preferential treatment. Implementing QoS in your wireless LAN makes network performance more predictable and bandwidth utilization more effective.

When you configure QoS, you create QoS policies and apply the policies to the VLAN configured on your access point/bridge. If you do not use VLANs on your network, you can apply your QoS policies to the access point/bridge's Ethernet and radio ports.

**Note**

When you enable QoS, the access point uses Wi-Fi Multimedia (WMM) mode by default. See the [“Using Wi-Fi Multimedia Mode” section on page 14-4](#) for information on WMM.

QoS for Wireless LANs Versus QoS on Wired LANs

The QoS implementation for wireless LANs differs from QoS implementations on other Cisco devices. With QoS enabled, access points perform the following:

- They do not classify packets; they prioritize packets based on DSCP value, client type (such as a wireless phone), or the priority value in the 802.1q or 802.1p tag.
- They do not construct internal DSCP values; they only support mapping by assigning IP DSCP, Precedence, or Protocol values to Layer 2 COS values.
- They carry out EDCF like queuing on the radio egress port only.
- They do only FIFO queueing on the Ethernet egress port.
- They support only 802.1Q/P tagged packets. Access points do not support ISL.
- They support only MQC policy-map **set cos** action.
- They prioritize the traffic from voice clients (such as Symbol phones) over traffic from other clients when the QoS Element for Wireless Phones feature is enabled.
- They support Spectralink phones using the class-map IP protocol clause with the protocol value set to 119.

To contrast the wireless LAN QoS implementation with the QoS implementation on other Cisco network devices, see the *Cisco IOS Quality of Service Solutions Configuration Guide* at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_c/index.htm

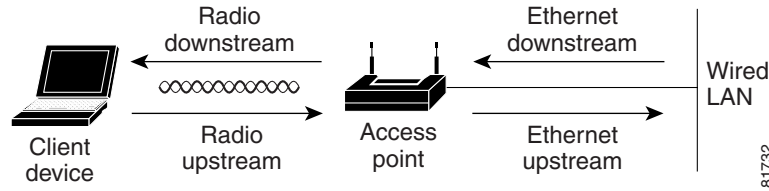
Impact of QoS on a Wireless LAN

Wireless LAN QoS features are a subset of the proposed 802.11e draft. QoS on wireless LANs provides prioritization of traffic from the access point/bridge over the WLAN based on traffic classification.

Just as in other media, you might not notice the effects of QoS on a lightly loaded wireless LAN. The benefits of QoS become more obvious as the load on the wireless LAN increases, keeping the latency, jitter, and loss for selected traffic types within an acceptable range.

QoS on the wireless LAN focuses on downstream prioritization from the access point. Figure 14-1 shows the upstream and downstream traffic flow.

Figure 14-1 Upstream and Downstream Traffic Flow



QoS on the wireless LAN focuses on downstream prioritization from the access point/bridge. These are the effects of QoS on access point/bridge traffic:

- The radio downstream flow is traffic transmitted out the access point/bridge radio to a wireless client device. This traffic is the main focus for QoS on a wireless LAN.
- The radio upstream flow is traffic transmitted out the wireless client device to the access point/bridge. QoS for wireless LANs does not affect this traffic.
- The Ethernet downstream flow is traffic sent from a switch or a router to the Ethernet port on the access point/bridge. If QoS is enabled on the switch or router, the switch or router might prioritize and rate-limit traffic to the access point.
- The Ethernet upstream flow is traffic sent from the access point/bridge Ethernet port to a switch or router on the wired LAN. The access point/bridge does not prioritize traffic that it sends to the wired LAN based on traffic classification.

Precedence of QoS Settings

When you enable QoS, the access point/bridge queues packets based on the Layer 2 class of service value for each packet. The access point/bridge applies QoS policies in this order:

1. **Packets already classified**—When the access point/bridge receives packets from a QoS-enabled switch or router that has already classified the packets with non-zero 802.1Q/P user_priority values, the access point/bridge uses that classification and does not apply other QoS policy rules to the packets. An existing classification takes precedence over all other policies on the access point/bridge.



Note Even if you have not configured a QoS policy, the access point always honors tagged 802.1P packets that it receives over the radio interface.

2. **QoS Element for Wireless Phones setting**—If you enable the *QoS Element for Wireless Phones* setting, dynamic voice classifiers are created for some of the wireless phone vendor clients, which allows the wireless phone traffic to be a higher priority than other clients' traffic. Additionally, the QoS Basic Service Set (QBSS) is enabled to advertise channel load information in the beacon and probe response frames. Some IP phones use QBSS elements to determine which access point to associate to, based on the traffic load.

You can use the Cisco IOS command **dot11 phone dot11e** command to enable the future upgrade of the 7920 Wireless Phone firmware to support the standard QBSS Load IE. The new 7920 Wireless Phone firmware will be announced at a later date.

**Note**

This release continues to support existing 7920 wireless phone firmware. Do not attempt to use the new standard (IEEE 802.11e draft 13) QBSS Load IE with the 7920 Wireless Phone until new phone firmware is available for you to upgrade your phones.

This example shows how to enable IEEE 802.11 phone support with the legacy QBSS Load element:

```
AP(config)# dot11 phone
```

This example shows how to enable IEEE 802.11 phone support with the standard (IEEE 802.11e draft 13) QBSS Load element:

```
AP(config)# no dot11 phone dot11e
```

This example shows how to stop or disable the IEEE 802.11 phone support:

```
AP(config)# no dot11 phone
```

3. Policies you create on the access point/bridge—QoS Policies that you create and apply to VLANs or to the access point/bridge interfaces are second in precedence after previously classified packets.
4. Default classification for all packets on VLAN—If you set a default classification for all packets on a VLAN, that policy is third in the precedence list.

Using Wi-Fi Multimedia Mode

When you enable QoS, the access point uses Wi-Fi Multimedia (WMM) mode by default. WMM provides these enhancements over basic QoS mode:

- The access point adds each packet's class of service to the packet's 802.11 header to be passed to the receiving station.
- Each access class has its own 802.11 sequence number. The sequence number allows a high-priority packet to interrupt the retries of a lower-priority packet without overflowing the duplicate checking buffer on the receiving side.
- WPA replay detection is done per access class on the receiver. Like 802.11 sequence numbering, WPA replay detection allows high-priority packets to interrupt lower priority retries without signalling a replay on the receiving station.
- For access classes that are configured to allow it, transmitters that are qualified to transmit through the normal backoff procedure are allowed to send a set of pending packets during the configured transmit opportunity (a specific number of microseconds). Sending a set of pending packets improves throughput because each packet does not have to wait for a backoff to gain access; instead, the packets can be transmitted immediately one after the other.

The access point uses WMM enhancements in packets sent to client devices that support WMM. The access point applies basic QoS policies to packets sent to clients that do not support WMM.

Use the **no dot11 qos mode wmm** configuration interface command to disable WMM using the CLI. To disable WMM using the web-browser interface, unselect the check boxes for the radio interfaces on the QoS Advanced page. [Figure 14-4](#) shows the QoS Advanced page.

Configuring QoS

QoS is disabled by default (however, the radio interface always honors tagged 802.1P packets even when you have not configured a QoS policy). This section describes how to configure QoS on your access point. It contains this configuration information:

- [Configuration Guidelines, page 14-5](#)
- [Configuring QoS Using the Web-Browser Interface, page 14-5](#)
- [Adjusting Radio Access Category Definitions, page 14-9](#)
- [“Disabling IGMP Snooping Helper” section on page 14-11](#)
- [“Disabling AVVID Priority Mapping” section on page 14-11](#)

Configuration Guidelines

Before configuring QoS on your access point/bridge, you should be aware of this information:

- The most important guideline in QoS deployment is to be familiar with the traffic on your wireless LAN. If you know the applications used by wireless client devices, the applications' sensitivity to delay, and the amount of traffic associated with the applications, you can configure QoS to improve performance.
- QoS does not create additional bandwidth for your wireless LAN; it helps control the allocation of bandwidth. If you have plenty of bandwidth on your wireless LAN, you might not need to configure QoS.

Configuring QoS Using the Web-Browser Interface

This section describes configuring QoS using the web-browser interface.

For a list of IOS commands for configuring QoS using the CLI, consult the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*. Follow these steps to browse to the command reference:

1. Click this link to browse to the Cisco Aironet documentation home page:
<http://www.cisco.com/univercd/cc/td/doc/product/wireless/index.htm>
2. Follow this path to the product, document, and chapter:
Products & Solutions > Wireless > All Wireless Products > Cisco Aironet 1300 Series > Technical Documentation > Command References > Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges, 12.x(xx)JA

Follow these steps to configure QoS:

This section describes configuring QoS using the web-browser interface.

For a list of Cisco IOS commands for configuring QoS using the CLI, consult the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*.

Follow these steps to configure QoS:

-
- Step 1** If you use VLANs on your wireless LAN, make sure the necessary VLANs are configured on your access point before configuring QoS.

- Step 1** Click **Services** in the task menu on the left side of any page in the web-browser interface. When the list of Services expands, click **QoS**. The QoS Policies page appears. Figure 14-2 shows the QoS Policies page.

Figure 14-2 QoS Policies Page

Cisco Aironet 1300 Series Wireless Bridge

QoS POLICIES | RADIO0-802.11G ACCESS CATEGORIES | ADVANCED

Hostname repeater | repeater uptime is 6 days, 23 hours, 47 minutes

Services: QoS Policies

Create/Edit Policies

Create/Edit Policy:

Policy Name:

Classifications:

Match Classifications:

IP Precedence:

IP DSCP: ☒ Best Effort ☐

IP Protocol 119:

Filter: No Filters defined. [Define Filters](#)

Default Classification for Packets on the VLAN:

Apply Policies to Interface/ VLANs

VLAN 1	FastEthernet	Radio0-802.11G
Incoming	NONE	NONE
Outgoing	NONE	NONE

VLAN 71	FastEthernet	Radio0-802.11G
Incoming	NONE	NONE
Outgoing	NONE	NONE

- Step 2** With **<NEW>** selected in the Create/Edit Policy field, type a name for the QoS policy in the Policy Name entry field. The name can contain up to 25 alphanumeric characters. Do not include spaces in the policy name.

- Step 3** If the packets that you need to prioritize contain IP precedence information in the IP header TOS field, select an IP precedence classification from the IP Precedence drop-down menu. Menu selections include:
- Routine (0)
 - Priority (1)
 - Immediate (2)
 - Flash (3)
 - Flash Override (4)
 - Critic/CCP (5)
 - Internet Control (6)
 - Network Control (7)
- Step 4** Use the Apply Class of Service drop-down menu to select the class of service that the access point will apply to packets of the type that you selected from the IP Precedence menu. The access point matches your IP Precedence selection with your class of service selection. Settings in the Apply Class of Service menu include:
- Best Effort (0)
 - Background (1)
 - Spare (2)
 - Excellent (3)
 - Control Lead (4)
 - Video <100ms Latency (5)
 - Voice <100ms Latency (6)
 - Network Control (7)
- Step 5** Click the **Add** button beside the Class of Service menu for IP Precedence. The classification appears in the Classifications field. To delete a classification, select it and click the **Delete** button beside the Classifications field.
- Step 6** If the packets that you need to prioritize contain IP DSCP precedence information in the IP header TOS field, select an IP DSCP classification from the IP DSCP drop-down menu. Menu selections include:
- Best Effort
 - Assured Forwarding — Class 1 Low
 - Assured Forwarding — Class 1 Medium
 - Assured Forwarding — Class 1 High
 - Assured Forwarding — Class 2 Low
 - Assured Forwarding — Class 2 Medium
 - Assured Forwarding — Class 2 High
 - Assured Forwarding — Class 3 Low
 - Assured Forwarding — Class 3 Medium
 - Assured Forwarding — Class 3 High
 - Assured Forwarding — Class 4 Low
 - Assured Forwarding — Class 4 Medium
 - Assured Forwarding — Class 4 High

- Class Selector 1
- Class Selector 2
- Class Selector 3
- Class Selector 4
- Class Selector 5
- Class Selector 6
- Class Selector 7
- Expedited Forwarding

- Step 7** Use the Apply Class of Service drop-down menu to select the class of service that the access point will apply to packets of the type that you selected from the IP DSCP menu. The access point matches your IP DSCP selection with your class of service selection.
- Step 8** Click the **Add** button beside the Class of Service menu for IP DSCP. The classification appears in the Classifications field.
- Step 9** If you need to prioritize the packets from Spectralink phones (IP Protocol 119) on your wireless LAN, use the Apply Class of Service drop-down menu to select the class of service that the access point will apply to Spectralink phone packets. The access point matches Spectralink phone packets with your class of service selection.
- Step 10** Click the **Add** button beside the Class of Service menu for IP Protocol 119. The classification appears in the Classifications field.
- Step 11** If you need to assign a priority to filtered packets, use the Filter drop-down menu to select a Filter to include in the policy. (If no filters are defined on the access point, a link to the Apply Filters page appears instead of the Filter drop-down menu.) For example, you could assign a high priority to a MAC address filter that includes the MAC addresses of IP phones.



Note The access list you use in QoS does not affect the access points' packet forwarding decisions.

- Step 12** Use the Apply Class of Service drop-down menu to select the class of service that the access point will apply to packets that match the filter that you selected from the Filter menu. The access point matches your filter selection with your class of service selection.
- Step 13** Click the **Add** button beside the Class of Service menu for Filter. The classification appears in the Classifications field.
- Step 14** If you want to set a default classification for all packets on a VLAN, use the Apply Class of Service drop-down menu to select the class of service that the access point will apply to all packets on a VLAN. The access point matches all packets with your class of service selection.
- Step 15** Click the **Add** button beside the Class of Service menu for *Default classification for packets on the VLAN*. The classification appears in the Classifications field.
- Step 16** When you finish adding classifications to the policy, click the **Apply** button under the Apply Class of Service drop-down menus. To cancel the policy and reset all fields to defaults, click the **Cancel** button under the Apply Class of Service drop-down menus. To delete the entire policy, click the **Delete** button under the Apply Class of Service drop-down menus.
- Step 17** Use the Apply Policies to Interface/VLANs drop-down menus to apply policies to the access point Ethernet and radio ports. If VLANs are configured on the access point, drop-down menus for each VLANs' virtual ports appear in this section. If VLANs are not configured on the access point, drop-down menus for each interface appear.

Step 18 Click the **Apply** button at the bottom of the page to apply the policies to the access point ports.

If you want the access point to give priority to all voice packets regardless of VLAN, click the **Advanced** tab. Figure 14-3 shows the QoS Policies - Advanced page.

Figure 14-3 QoS Policies - Advanced Page

HOME
EXPRESS SET-UP
EXPRESS SECURITY
NETWORK MAP +
ASSOCIATION +
NETWORK INTERFACES +
SECURITY +
SERVICES
Telnet/SSH
Hot Standby
CDP
DNS
Filters
HTTP
QoS
SNMP
SNTP
VLAN
ARP Caching
WIRELESS SERVICES +
SYSTEM SOFTWARE +
EVENT LOG +

QoS POLICIES RADIO0-802.11G ACCESS CATEGORIES RADIO1-802.11A ACCESS CATEGORIES ADVANCED

Hostname AP1242AG AP1242AG uptime is 1 hour, 13 minutes

Services: QoS Policies - Advanced

IP Phone

QoS Element for Wireless Phones : ☒ Enable ☐ Dot11e
☐ Disable

IGMP Snooping

Snooping Helper: ☒ Enable ☐ Disable

AVVID Priority Mapping

Map Ethernet Packets with CoS 5 to CoS 6: ☐ Yes ☒ No

WiFi MultiMedia (WMM)

Enable on Radio Interfaces:

☒ Radio0-802.11G
☒ Radio1-802.11A

Apply Cancel

121642

Select **Enable** and click **Apply** to give top priority to all voice packets.



Note Click **dot11e** to use the latest version of QBSS Load IE. If you do click **dot11e**, the previous version QBSS Load IE is used.



Note When you enable QoS Element for Wireless Phones, the access point gives top priority to voice packets even if you do not enable QoS. This setting operates independently from the QoS policies that you configure.

Adjusting Radio Access Category Definitions

The access point uses the radio access categories to calculate backoff times for each packet. As a rule, high-priority packets have short backoff times.

The default values in the Min and Max Contention Window fields and in the Slot Time fields are based on settings recommended in IEEE Draft Standard 802.11e. For detailed information on these values, consult that standard.

Cisco strongly recommends that you use the default settings on the Radio Access Categories page. Changing these values can lead to unexpected blockages of traffic on your wireless LAN, and the blockages might be difficult to diagnose. If you change these values and find that you need to reset them to defaults, use the default settings listed in [Table 14-1](#).

The values listed in [Table 14-1](#) are to the power of 2. The access point computes Contention Window values with this equation:

$$CW = 2^{**} X \text{ minus } 1$$

where X is the value from [Table 14-1](#).

Table 14-1 Default QoS Radio Access Categories

Class of Service	Min Contention Window	Max Contention Window	Fixed Slot Time	Transmit Opportunity
Background	4	10	6	0
Best Effort	4	10	2	0
Video <100ms Latency	3	2	1	3008
Voice <100ms Latency	2	3	1	1504

[Figure 14-4](#) shows the Radio 802.11G Access Categories page.

Figure 14-4 Radio 802.11G Access Categories Page



Note

In this release, clients are blocked from using an access category when you select **Enable** for Admission Control.

Using the Admission Control check boxes, you can control client use of the access categories. When you enable admission control for an access category, clients associated to the access point must complete the WMM admission control procedure before they can use that access category. However, access points do not support the admission control procedure in this release, so clients cannot use the access category when you enable Admission Control.

Disabling IGMP Snooping Helper

When Internet Group Membership Protocol (IGMP) snooping is enabled on a switch and a client roams from one access point to another, the clients' multicast session is dropped. When the access points' IGMP snooping helper is enabled, the access point sends a general IGMP query to the network infrastructure on behalf of the client every time the client associates or reassociates to the access point. By doing so, the multicast stream is maintained for the client as it roams.

The IGMP snooping helper is enabled by default. To disable it, browse to the QoS Policies - Advanced page, select **Disable**, and click **Apply**. Figure 14-3 shows the QoS Policies - Advanced page.

Disabling AVVID Priority Mapping

AVVID priority mapping maps Ethernet packets tagged as class of service 5 to class of service 6. This feature enables the access point to apply the correct priority to voice packets for compatibility with Cisco AVVID networks.

AVVID priority mapping is enabled by default. To disable it, browse to the QoS Policies - Advanced page, select **No** for Map Ethernet Packets with CoS 5 to CoS 6, and click **Apply**. Figure 14-3 shows the QoS Policies - Advanced page.

CW-min and CW-max Settings for Point-to-Point and Point-to-Multipoint Bridge Links

For best performance on your bridge links, adjust the CW-min and CW-max contention window settings according to the values listed in Table 14-2. The default settings, CW-min 3 and CW-max 10, are best for point-to-point links. However, for point-to-multipoint links, you should adjust the settings depending on the number of non-root bridges that associate to the root bridge.



Note If packet concatenation is enabled, you need to adjust the CW-min and CW-max settings only for traffic class 0. Concatenation is enabled by default.

Table 14-2 CW-min and CW-max Settings for Point-to-Point and Point-to-Multipoint Bridge Links

Setting	Point-to-Point Links	Point-to-Multipoint Links with up to 5 Non-Root Bridges	Point-to-Multipoint Links with up to 10 Non-Root Bridges	Point-to-Multipoint Links with up to 17 Non-Root Bridges
CW-min	3	4	5	6
CW-max	10	10	10	10

Beginning in privileged EXEC mode, follow these steps to adjust the CW-min and CW-max settings:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.
Step 3	traffic class { cw-min number } { cw-max number } { fixed-slot number }	Assign CW-min, CW-max, and fixed-slot settings to a traffic class. Use the values in Table 14-2 to enter settings that provide the best performance for your network configuration. Note If packet concatenation is enabled, you need to adjust the CW-min and CW-max settings only for traffic class 0. Concatenation is enabled by default.
Step 4	end	Return to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Use the **no** form of the command to reset the setting to defaults.

QoS Configuration Examples

These sections describe two common uses for QoS:

- [Giving Priority to Voice Traffic, page 14-12](#)
- [Giving Priority to Video Traffic, page 14-13](#)

Giving Priority to Voice Traffic

This section demonstrates how you can apply a QoS policy to your wireless network's voice VLAN to give priority to wireless phone traffic.

In this example, the network administrator creates a policy named *voice_policy* that applies voice class of service to traffic from Spectralink phones (protocol 119 packets). The user applies the *voice_policy* to the incoming and outgoing radio ports and to the outgoing Ethernet port for VLAN 77. [Figure 14-5](#) shows the administrator's QoS Policies page.

Figure 14-5 QoS Policies Page for Voice Example

HOME
EXPRESS SET-UP
EXPRESS SECURITY
NETWORK MAP +
ASSOCIATION +
NETWORK INTERFACES +
SECURITY +
SERVICES
Telnet/SSH
CDP
DNS
Filters
HTTP
Proxy Mobile IP
QoS
SNMP
NTP
VLAN
STP
ARP Caching
WIRELESS SERVICES +
SYSTEM SOFTWARE +
EVENT LOG +

QoS POLICIES RADIO0-802.11G ACCESS CATEGORIES ADVANCED

Hostname bridge bridge uptime is 1 day, 23 hours, 55 minutes

Services: QoS Policies

Create/Edit Policies

Create/Edit Policy: voice_policy

Policy Name: voice_policy

Classifications: Precedence Priority - COS Voice < 10ms Latency (6)

Delete Classification

Match Classifications:

IP Precedence: Routine (0)

IP DSCP: Best Effort (0-63)

IP Protocol 119

Filter: No Filters defined. [Define Filters.](#)

Apply Class of Service

Best Effort (0) Add

Best Effort (0) Add

Best Effort (0) Add

Apply Delete Cancel

Apply Policies to Interface/ VLANs

	FastEthernet	Radio0-802.11G
Incoming	< NONE >	voice_policy
Outgoing	voice_policy	voice_policy

Apply Cancel

The network administrator also enables the *QoS element for wireless phones* setting on the QoS Policies - Advanced page. This setting gives priority to all voice traffic regardless of VLAN.

Giving Priority to Video Traffic

This section demonstrates how you could apply a QoS policy to a VLAN on your network dedicated to video traffic.

In this example, the network administrator creates a policy named *video_policy* that applies video class of service to video traffic. The user applies the *video_policy* to the incoming and outgoing radio ports and to the outgoing Ethernet port for VLAN 87. Figure 14-6 shows the administrator's QoS Policies page.

Figure 14-6 QoS Policies Page for Video Example

HOME
EXPRESS SET-UP
EXPRESS SECURITY
NETWORK MAP
ASSOCIATION
NETWORK INTERFACES
SECURITY
SERVICES
Telnet/SSH
CDP
DNS
Filters
HTTP
Proxy Mobile IP
QoS
SNMP
NTP
VLAN
STP
ARP Caching
WIRELESS SERVICES
SYSTEM SOFTWARE
EVENT LOG

QoS POLICIES

RADIO0-802.11G
ACCESS CATEGORIES

ADVANCED

Hostname bridge
bridge uptime is 2 days, 0 minutes

Services: QoS Policies

Create/Edit Policies

Create/Edit Policy: video_policy

Policy Name: video_policy

Classifications: Precedence Routine - COS Video <100ms Latency (5)

Delete Classification

Match Classifications:

IP Precedence: Routine (0)

IP DSCP: Best Effort (0-63)

IP Protocol 119

Filter: No Filters defined. [Define Filters.](#)

Apply Class of Service

Video <100ms Latency (5)

Best Effort (0)

Best Effort (0)

Add

Add

Add

Apply

Delete

Cancel

Apply Policies to Interface/ VLANs

	FastEthernet	Radio0-802.11G
Incoming	< NONE >	video_policy
Outgoing	video_policy	video_policy

Apply

Cancel

117030



Configuring Filters

This chapter describes how to configure and manage MAC address, IP, and Ethertype filters on the access point/bridge using the web-browser interface. This chapter contains these sections:

- [Understanding Filters, page 15-2](#)
- [Configuring Filters Using the CLI, page 15-2](#)
- [Configuring Filters Using the Web-Browser Interface, page 15-2](#)

Understanding Filters

Protocol filters (IP protocol, IP port, and EtherType) prevent or allow the use of specific protocols through the access point/bridge's Ethernet and radio ports. 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/bridge's radio port prevents wireless clients from using SNMP with the access point/bridge but does not block SNMP access from the wired LAN.

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

You can configure filters using the web-browser interface or by entering commands in the CLI.



Tip

You can include filters in the access point/bridge's QoS policies. Refer to [Chapter 14, “Configuring QoS,”](#) for detailed instructions on setting up QoS policies.

Configuring Filters Using the CLI

To configure filters using IOS commands, you use access control lists (ACLs) and access point/bridge groups. You can find explanations of these concepts and instructions for implementing them in these documents:

- *Cisco IOS Bridging and IBM Networking Configuration Guide, Release 12.2.* Click this link to browse to the “Configuring Transparent Bridging” chapter:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fibm_c/bcftb.htm
- *Catalyst 4908G-L3 Cisco IOS Release 12.0(10)W5(18e) Software Feature and Configuration Guide.* Click this link to browse to the “Command Reference” chapter:
http://www.cisco.com/univercd/cc/td/doc/product/13sw/4908g_13/ios_12/10w518e/config/cmd_ref.htm

Configuring Filters Using the Web-Browser Interface

This section describes how to configure and enable filters using the web-browser interface. You complete two steps to configure and enable a filter:

1. Name and configure the filter using the filter setup pages.
2. Enable the filter using the Apply Filters page.

These sections describe setting up and enabling three filter types:

- [Configuring and Enabling MAC Address Filters, page 15-3](#)
- [Configuring and Enabling IP Filters, page 15-7](#)
- [Configuring and Enabling EtherType Filters, page 15-10](#)

Configuring and Enabling MAC Address Filters

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. You can apply the filters you create to either or both the Ethernet and radio ports and to either or both incoming and outgoing packets.



Note

Using the CLI, you can configure up to 2,048 MAC addresses for filtering. Using the web browser interface, you can configure only up to 43 MAC address for filtering.



Note

MAC address filters are powerful, and you can lock yourself out of the access point/bridge if you make a mistake setting up the filters. If you accidentally lock yourself out of your access point/bridge, use the CLI to disable the filters, or use the Mode button on the access point/bridge power injector to reset the access point/bridge to factory defaults.

Use the MAC Address Filters page to create MAC address filters for the access point/bridge. [Figure 15-1](#) shows the MAC Address Filters page.

Figure 15-1 *MAC Address Filters Page*

Follow this link path to reach the Address Filters page:

1. Click **Services** in the page navigation bar.
2. In the Services page list, click **Filters**.
3. On the Apply Filters page, click the **MAC Address Filters** tab at the top of the page.

Creating a MAC Address Filter

Follow these steps to create a MAC address filter:

-
- Step 1** Follow the link path to the MAC Address Filters page.
- Step 2** If you are creating a new MAC address filter, make sure **<NEW>** (the default) is selected in the Create/Edit Filter Index menu. To edit a filter, select the filter number from the Create/Edit Filter Index menu.
- Step 3** In the Filter Index field, name the filter with a number from 700 to 799. The number you assign creates an access control list (ACL) for the filter.
- Step 4** Enter a MAC address in the Add MAC Address field. Enter the address with periods separating the three groups of four characters (0005.9a39.3456, for example).



Note To make sure the filter operates properly, use lower case for all the letters in the MAC address that you enter.

- Step 5** Use the Mask entry field to indicate how many bits, from left to right, the filter checks against the MAC address. For example, to require an exact match with the MAC address (to check all bits) enter **0000.0000.0000**. To check only the first 4 bytes, enter **0.0.FFFF**.
- Step 6** Select **Forward** or **Block** from the Action menu.
- Step 7** Click **Add**. The MAC address appears in the Filters Classes field. To remove the MAC address from the Filters Classes list, select it and click **Delete Class**.
- Step 8** Repeat [Step 4](#) through [Step 7](#) to add addresses to the filter.
- Step 9** Select **Forward All** or **Block All** from the Default Action menu. The filter's default action must be the opposite of the action for at least one of the addresses in the filter. For example, if you enter several addresses and you select **Block** as the action for all of them, you must choose **Forward All** as the filter's default action.



Tip You can create a list of allowed MAC addresses on an authentication server on our network. Consult the [Chapter 10, "Configuring Authentication Types"](#) for instructions on using MAC based authentication.

- Step 10** Click **Apply**. The filter is saved on the access point/bridge, but it is not enabled until you apply it on the Apply Filters page.
- Step 11** Click the **Apply Filters** tab to return to the Apply Filters page. [Figure 15-2](#) shows the Apply Filters page.

Figure 15-2 Apply Filters Page

		FastEthernet		Radio0-802.11G	
Incoming	MAC	< NONE >		MAC	< NONE >
	EtherType	< NONE >		EtherType	< NONE >
	IP	< NONE >		IP	< NONE >
Outgoing	MAC	< NONE >		MAC	< NONE >
	EtherType	< NONE >		EtherType	< NONE >
	IP	< NONE >		IP	< NONE >

Step 12 Select the filter number from one of the MAC drop-down menus. You can apply the filter to either or both the Ethernet and radio ports, and to either or both incoming and outgoing packets.

Step 13 Click **Apply**. The filter is enabled on the selected ports.

If clients are not filtered immediately, click **Reload** on the System Configuration page to restart the access point/bridge. To reach the System Configuration page, click **System Software** on the task menu and then click **System Configuration**.

Using MAC Address ACLs to Block or Allow Client Association to the Access Point

You can use MAC address ACLs to block or allow association to the access point. Instead of filtering traffic across an interface, you use the ACL to filter associations to the access point radio.

Follow these steps to use an ACL to filter associations to the access point radio:

- Step 1** Follow Steps 1 through 10 in the “[Creating a MAC Address Filter](#)” section on page 15-4 to create an ACL. For MAC addresses that you want to allow to associate, select **Forward** from the Action menu. Select **Block** for addresses that you want to prevent from associating. Select **Block All** from the Default Action menu.
- Step 2** Click **Security** to browse to the Security Summary page. [Figure 15-3](#) shows the Security Summary page.

Figure 15-3 Security Summary Page


Cisco Aironet 1300 Series Wireless Bridge

Hostname root root uptime is 1 week, 1 hour, 27 minutes

HOME

EXPRESS SET-UP

EXPRESS SECURITY

NETWORK MAP +

ASSOCIATION +

NETWORK INTERFACES +

SECURITY

Admin Access

Encryption Manager

SSID Manager

Server Manager

Local RADIUS Server

Advanced Security

SERVICES +

WIRELESS SERVICES +

SYSTEM SOFTWARE +

EVENT LOG +

Security Summary

[Administrators](#)

Username	Read-Only	Read-Write
Cisco	✓	

[Service Set Identifiers \(SSIDs\)](#)

SSID	VLAN	Radio	BSSID/Guest Mode	Open	Shared	Network EAP
floorine	1	Radio0-802.11G	0012.433d.f400	no addition		
vlan71	71	Radio0-802.11G	0012.433d.f400 ✓	no addition		

[Encryption Settings](#)

VLAN	Encryption Mode	WEP		Cipher						Key Rotation
		MIC	PPK	TKIP	WEP40bit	WEP128bit	CKIP	CMIC	AES CCM	
1	None									
71	None									

[Server-Based Security](#)

Server Name/IP Address	Type	EAP	MAC	Admin	Accounting
192.168.170.2	RADIUS	✓			

Step 3 Click **Advanced Security** to browse to the Advanced Security: MAC Address Authentication page. [Figure 15-4](#) shows the MAC Address Authentication page.

Figure 15-4 Advanced Security: MAC Address Authentication Page


Cisco Aironet 1300 Series Wireless Bridge

Hostname root root uptime is 1 week, 1 hour, 32 minutes

HOME

EXPRESS SET-UP

EXPRESS SECURITY

NETWORK MAP +

ASSOCIATION +

NETWORK INTERFACES +

SECURITY

Admin Access

Encryption Manager

SSID Manager

Server Manager

Advanced Security

SERVICES +

WIRELESS SERVICES +

SYSTEM SOFTWARE +

EVENT LOG +

MAC ADDRESS AUTHENTICATION TIMERS ASSOCIATION ACCESS LIST

Security: Advanced Security- MAC Address Authentication

MAC Address Authentication

MAC Addresses Authenticated by:

☒ Local List Only
☐ Authentication Server Only
☐ Authentication Server if not found in Local List

Apply Cancel

Local MAC Address List

Local List:

Delete

New MAC Address: (HHHH.HHHH.HHHH)

Apply

- Step 4** Click the **Association Access List** tab to browse to the Association Access List page. [Figure 15-5](#) shows the Association Access List page.

Figure 15-5 Association List Page



- Step 5** Select your MAC address ACL from the drop down menu.
- Step 6** Click **Apply**.

This example shows the CLI commands that are equivalent to the steps listed in the “[Using MAC Address ACLs to Block or Allow Client Association to the Access Point](#)” section on page 15-5:

```
ap# configure terminal
ap(config)# dot11 association access-list 777
ap(config)# end
```

In this example, only client devices with MAC addresses listed in access list 777 are allowed to associate to the access point. The access point blocks associations from all other MAC addresses.

For complete descriptions of the commands used in this example, consult the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*.

Configuring and Enabling IP Filters

IP filters (IP address, IP protocol, and IP port) prevent or allow the use of specific protocols through the access point/bridge’s Ethernet and radio ports, and IP address filters allow or prevent the forwarding of unicast and multicast packets either sent from or addressed to specific IP addresses. You can create a filter that passes traffic to all addresses except those you specify, or you can create a filter that blocks traffic to all addresses except those you specify. You can create filters that contain elements of one, two, or all three IP filtering methods. You can apply the filters you create to either or both the Ethernet and radio ports and to either or both incoming and outgoing packets.

Use the IP Filters page to create IP filters for the access point/bridge. [Figure 15-6](#) shows the IP Filters page.

Figure 15-6 IP Filters Page

Hostname bridge bridge uptime is 1 day, 1 hour, 0 minutes

Services: Filters - IP Filters

Create/Edit Filter Name: <NEW>

Filter Name:

Default Action: Block All

IP Address

Destination Address: Mask: 0.0.0.0

Source Address: 0.0.0.0 Mask: 255.255.255.255

Action: Forward Add

IP Protocol

IP Protocol: ☒ Authentication Header Protocol (51) Action: Forward Add

☐ Custom (0-255)

UDP/TCP Port

TCP Port: ☒ Border Gateway Protocol (179) Action: Forward Add

☐ Custom (0-65535)

UDP Port: ☒ Biff (mail notification, comsat 512) Action: Forward Add

☐ Custom (0-65535)

Filters Classes

Delete Class

Apply Delete Cancel

Follow this link path to reach the IP Filters page:

1. Click **Services** in the page navigation bar.
2. In the Services page list, click **Filters**.
3. On the Apply Filters page, click the **IP Filters** tab at the top of the page.

Creating an IP Filter

Follow these steps to create an IP filter:

- Step 1** Follow the link path to the IP Filters page.
- Step 2** If you are creating a new filter, make sure <NEW> (the default) is selected in the Create/Edit Filter Index menu. To edit an existing filter, select the filter name from the Create/Edit Filter Index menu.
- Step 3** Enter a descriptive name for the new filter in the Filter Name field.

- Step 4** Select **Forward all** or **Block all** as the filter's default action from the Default Action menu. The filter's default action must be the opposite of the action for at least one of the addresses in the filter. For example, if you create a filter containing an IP address, an IP protocol, and an IP port and you select **Block** as the action for all of them, you must choose **Forward All** as the filter's default action.
- Step 5** To filter an IP address, enter an address in the IP Address field.
-  **Note** If you plan to block traffic to all IP addresses except those you specify as allowed, put the address of your own PC in the list of allowed addresses to avoid losing connectivity to the access point/bridge.
- Step 6** Type the mask for the IP address in the Mask field. Enter the mask with periods separating the groups of characters (112.334.556.778, for example). If you enter 255.255.255.255 as the mask, the access point/bridge accepts any IP address. If you enter 0.0.0.0, the access point/bridge looks for an exact match with the IP address you entered in the IP Address field. The mask you enter in this field behaves the same way that a mask behaves when you enter it in the CLI.
- Step 7** Select **Forward** or **Block** from the Action menu.
- Step 8** Click **Add**. The address appears in the Filters Classes field. To remove the address from the Filters Classes list, select it and click **Delete Class**. Repeat [Step 5](#) through [Step 8](#) to add addresses to the filter. If you do not need to add IP protocol or IP port elements to the filter, skip to [Step 15](#) to save the filter on the access point/bridge.
- Step 9** To filter an IP protocol, select one of the common protocols from the IP Protocol drop-down menu, or select the **Custom** radio button and enter the number of an existing ACL in the Custom field. Enter an ACL number from 0 to 255. See [Appendix A, "Protocol Filters,"](#) for a list of IP protocols and their numeric designators.
- Step 10** Select **Forward** or **Block** from the Action menu.
- Step 11** Click **Add**. The protocol appears in the Filters Classes field. To remove the protocol from the Filters Classes list, select it and click **Delete Class**. Repeat [Step 9](#) to [Step 11](#) to add protocols to the filter. If you do not need to add IP port elements to the filter, skip to [Step 15](#) to save the filter on the access point/bridge.
- Step 12** To filter a TCP or UDP port protocol, select one of the common port protocols from the TCP Port or UDP Port drop-down menus, or select the **Custom** radio button and enter the number of an existing protocol in one of the Custom fields. Enter a protocol number from 0 to 65535. See [Appendix A, "Protocol Filters,"](#) for a list of IP port protocols and their numeric designators.
- Step 13** Select **Forward** or **Block** from the Action menu.
- Step 14** Click **Add**. The protocol appears in the Filters Classes field. To remove the protocol from the Filters Classes list, select it and click **Delete Class**. Repeat [Step 12](#) to [Step 14](#) to add protocols to the filter.
- Step 15** When the filter is complete, click **Apply**. The filter is saved on the access point/bridge, but it is not enabled until you apply it on the Apply Filters page.
- Step 16** Click the **Apply Filters** tab to return to the Apply Filters page. [Figure 15-7](#) shows the Apply Filters page.

Figure 15-7 Apply Filters Page

Hostname bridge bridge uptime is 1 day, 23 hours, 30 minutes

Services: Filters - Apply Filters				
	FastEthernet		Radio0-802.11G	
Incoming	MAC	< NONE >	MAC	< NONE >
	EtherType	< NONE >	EtherType	< NONE >
	IP	< NONE >	IP	< NONE >
Outgoing	MAC	< NONE >	MAC	< NONE >
	EtherType	< NONE >	EtherType	< NONE >
	IP	< NONE >	IP	< NONE >

Apply Cancel

Step 17 Select the filter name from one of the IP drop-down menus. You can apply the filter to either or both the Ethernet and radio ports, and to either or both incoming and outgoing packets.

Step 18 Click **Apply**. The filter is enabled on the selected ports.

Configuring and Enabling Ethertype Filters

Ethertype filters prevent or allow the use of specific protocols through the access point/bridge's Ethernet and radio ports. You can apply the filters you create to either or both the Ethernet and radio ports and to either or both incoming and outgoing packets.

Use the Ethertype Filters page to create Ethertype filters for the access point/bridge. [Figure 15-8](#) shows the Ethertype Filters page.

Figure 15-8 *Ethertype Filters Page*

Hostname bridge bridge uptime is 1 day, 1 hour, 2 minutes

Services: Filters - EtherType Filters

Create/Edit Filter Index: <NEW>

Filter Index: (200-299)

Add EtherType: (0-FFFF) Mask: (0-FFFF) Action: Forward Add

Default Action: Block All

Filters Classes:

Delete Class

Apply Delete Cancel

Follow this link path to reach the Ethertype Filters page:

1. Click **Services** in the page navigation bar.
2. In the Services page list, click **Filters**.
3. On the Apply Filters page, click the **Ethertype Filters** tab at the top of the page.

Creating an Ethertype Filter

Follow these steps to create an Ethertype filter:

- Step 1** Follow the link path to the Ethertype Filters page.
- Step 2** If you are creating a new filter, make sure **<NEW>** (the default) is selected in the Create/Edit Filter Index menu. To edit an existing filter, select the filter number from the Create/Edit Filter Index menu.
- Step 3** In the Filter Index field, name the filter with a number from 200 to 299. The number you assign creates an access control list (ACL) for the filter.
- Step 4** Enter an Ethertype number in the Add Ethertype field. See [Appendix A, "Protocol Filters,"](#) for a list of protocols and their numeric designators.
- Step 5** Enter the mask for the Ethertype in the Mask field.
- Step 6** Select **Forward** or **Block** from the Action menu.
- Step 7** Click **Add**. The Ethertype appears in the Filters Classes field. To remove the Ethertype from the Filters Classes list, select it and click **Delete Class**. Repeat [Step 4](#) through [Step 7](#) to add Ethertypes to the filter.
- Step 8** Select **Forward All** or **Block All** from the Default Action menu. The filter's default action must be the opposite of the action for at least one of the Ethertypes in the filter. For example, if you enter several Ethertypes and you select **Block** as the action for all of them, you must choose **Forward All** as the filter's default action.

- Step 9** Click **Apply**. The filter is saved on the access point/bridge, but it is not enabled until you apply it on the Apply Filters page.
- Step 10** Click the **Apply Filters** tab to return to the Apply Filters page. [Figure 15-9](#) shows the Apply Filters page.

Figure 15-9 Apply Filters Page

Hostname bridge bridge uptime is 1 day, 23 hours, 30 minutes

Services: Filters - Apply Filters				
	FastEthernet		Radio0-802.11G	
Incoming	MAC	< NONE >	MAC	< NONE >
	EtherType	< NONE >	EtherType	< NONE >
	IP	< NONE >	IP	< NONE >
Outgoing	MAC	< NONE >	MAC	< NONE >
	EtherType	< NONE >	EtherType	< NONE >
	IP	< NONE >	IP	< NONE >

Apply Cancel

- Step 11** Select the filter number from one of the Ethertype drop-down menus. You can apply the filter to either or both the Ethernet and radio ports, and to either or both incoming and outgoing packets.
- Step 12** Click **Apply**. The filter is enabled on the selected ports.



Configuring CDP

This chapter describes how to configure Cisco Discovery Protocol (CDP) on your access point/bridge.



Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges* for this release and the *Cisco IOS Configuration Fundamentals Command Reference for Release 12.3*.

This chapter contains these sections:

- [Understanding CDP, page 16-2](#)
- [Configuring CDP, page 16-2](#)
- [Monitoring and Maintaining CDP, page 16-5](#)

Understanding CDP

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

CDP is enabled on the access points' Ethernet port by default. However, CDP is enabled on the access points' radio port only when the radio is associated to another wireless infrastructure device, such as an access point or a bridge.

**Note**

For best performance on your wireless LAN, disable CDP on all radio interfaces and on sub-interfaces if VLANs are enabled on the access point/bridge.

Configuring CDP

This section contains CDP configuration information and procedures:

- [Default CDP Configuration, page 16-2](#)
- [Configuring the CDP Characteristics, page 16-3](#)
- [Disabling and Enabling CDP, page 16-3](#)
- [Disabling and Enabling CDP on an Interface, page 16-4](#)

Default CDP Configuration

[Table 16-1](#) lists the default CDP settings.

Table 16-1 *Default CDP Configuration*

Feature	Default Setting
CDP global state	Enabled
CDP interface state	Enabled
CDP holdtime (packet holdtime in seconds)	180
CDP timer (packets sent every x seconds)	60

Configuring the CDP Characteristics

You can configure the CDP holdtime (the number of seconds before the access point/bridge discards CDP packets) and the CDP timer (the number of seconds between each CDP packets the access point/bridge sends).

Beginning in Privileged Exec mode, follow these steps to configure the CDP holdtime and CDP timer:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	cdp holdtime <i>seconds</i>	(Optional) Specify the amount of time a receiving device should hold the information sent by your device before discarding it. The range is from 10 to 255 seconds; the default is 180 seconds.
Step 3	cdp timer <i>seconds</i>	(Optional) Set the transmission frequency of CDP updates in seconds. The range is from 5 to 254; the default is 60 seconds.
Step 4	end	Return to Privileged Exec mode.

Use the **no** form of the CDP commands to return to the default settings.

This example shows how to configure and verify CDP characteristics:

```
ap# configure terminal
ap(config)# cdp holdtime 120
ap(config)# cdp timer 50
ap(config)# end

ap# show cdp

Global CDP information:
    Sending a holdtime value of 120 seconds
    Sending CDP packets every 50 seconds
```

For additional CDP **show** commands, see the [“Monitoring and Maintaining CDP”](#) section on page 16-5.

Disabling and Enabling CDP

CDP is enabled by default. Beginning in Privileged Exec mode, follow these steps to disable the CDP device discovery capability:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	no cdp run	Disable CDP.
Step 3	end	Return to Privileged Exec mode.

Beginning in privileged EXEC mode, follow these steps to enable CDP:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	cdp run	Enable CDP after disabling it.
Step 3	end	Return to privileged EXEC mode.

This example shows how to enable CDP.

```
ap# configure terminal
ap(config)# cdp run
ap(config)# end
```

Disabling and Enabling CDP on an Interface

CDP is enabled by default on all supported interfaces to send and receive CDP information.

Beginning in privileged EXEC mode, follow these steps to disable CDP on an interface:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface <i>interface-id</i>	Enter interface configuration mode, and enter the interface on which you are disabling CDP.
Step 3	no cdp enable	Disable CDP on an interface.
Step 4	end	Return to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Beginning in privileged EXEC mode, follow these steps to enable CDP on an interface:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface <i>interface-id</i>	Enter interface configuration mode, and enter the interface on which you are enabling CDP.
Step 3	cdp enable	Enable CDP on an interface after disabling it.
Step 4	end	Return to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to enable CDP on an interface:

```
ap# configure terminal
ap(config)# interface x
ap(config-if)# cdp enable
ap(config-if)# end
```

Monitoring and Maintaining CDP

To monitor and maintain CDP on your device, perform one or more of these tasks, beginning in privileged EXEC mode.

Command	Description
clear cdp counters	Reset the traffic counters to zero.
clear cdp table	Delete the CDP table of information about neighbors.
show cdp	Display global information, such as frequency of transmissions and the holdtime for packets being sent.
show cdp entry <i>entry-name</i> [protocol version]	Display information about a specific neighbor. You can enter an asterisk (*) to display all CDP neighbors, or you can enter the name of the neighbor about which you want information. You can also limit the display to information about the protocols enabled on the specified neighbor or information about the version of software running on the device.
show cdp interface [<i>type number</i>]	Display information about interfaces where CDP is enabled. You can limit the display to the type of interface or the number of the interface about which you want information (for example, entering gigabitethernet 0/1 displays information only about Gigabit Ethernet port 1).
show cdp neighbors [<i>type number</i>] [detail]	Display information about neighbors, including device type, interface type and number, holdtime settings, capabilities, platform, and port ID. You can limit the display to neighbors on a specific type or number of interface or expand the display to provide more detailed information.
show cdp traffic	Display CDP counters, including the number of packets sent and received and checksum errors.

Below are six examples of output from the CDP **show** privileged EXEC commands:

```
ap# show cdp
Global CDP information:
    Sending CDP packets every 50 seconds
    Sending a holdtime value of 120 seconds

ap# show cdp entry *
-----
Device ID: ap
Entry address(es):
    IP address: 10.1.1.66
Platform: cisco WS-C3550-12T, Capabilities: Switch IGMP
Interface: GigabitEthernet0/2, Port ID (outgoing port): GigabitEthernet0/2
Holdtime : 129 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) C3550 Software (C3550-I5Q3L2-M), Experimental Version 12.1(20010612:021
316) [jang-flamingo 120]
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Fri 06-Jul-01 18:18 by jang

advertisement version: 2
```

```

Protocol Hello:  OUI=0x00000C, Protocol ID=0x0112; payload len=27, value=0000000
0FFFFFFF010221FF0000000000000024B293A00FF0000
VTP Management Domain:  ''
Duplex: full

```

```

-----
Device ID: idf2-1-lab-13.cisco.com
Entry address(es):
  IP address: 10.1.1.10
Platform: cisco WS-C3524-XL, Capabilities: Trans-Bridge Switch
Interface: GigabitEthernet0/1, Port ID (outgoing port): FastEthernet0/10
Holdtime : 141 sec

```

```

Version :
Cisco Internetwork Operating System Software
IOS (tm) C3500XL Software (C3500XL-C3H2S-M), Version 12.0(5.1)XP, MAINTENANCE IN
TERIM SOFTWARE
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Fri 10-Dec-99 11:16 by cchang

```

```

advertisement version: 2
Protocol Hello:  OUI=0x00000C, Protocol ID=0x0112; payload len=25, value=0000000
0FFFFFFF010101FF000000000000000142EFA400FF
VTP Management Domain:  ''

```

```

ap# show cdp entry * protocol
Protocol information for talSwitch14 :
  IP address: 172.20.135.194
Protocol information for tstswitch2 :
  IP address: 172.20.135.204
  IP address: 172.20.135.202
Protocol information for tstswitch2 :
  IP address: 172.20.135.204
  IP address: 172.20.135.202

```

```

ap# show cdp interface
GigabitEthernet0/1 is up, line protocol is up
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
GigabitEthernet0/2 is up, line protocol is down
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
GigabitEthernet0/3 is administratively down, line protocol is down
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
GigabitEthernet0/4 is up, line protocol is down
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
GigabitEthernet0/5 is up, line protocol is up
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
GigabitEthernet0/6 is up, line protocol is up
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
GigabitEthernet0/7 is up, line protocol is down
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds

```

```
GigabitEthernet0/8 is up, line protocol is down
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
```

```
ap# show cdp neighbor
```

```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater
```

```
Device IDLocal InterfaceHoldtmeCapabilityPlatformPort ID
Perdido2Gig 0/6125R S IWS-C3550-1Gig0/6
Perdido2Gig 0/5125R S IWS-C3550-1Gig 0/5
```

```
ap# show cdp traffic
```

```
CDP counters :
```

```
Total packets output: 50882, Input: 52510
Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
No memory: 0, Invalid packet: 0, Fragmented: 0
CDP version 1 advertisements output: 0, Input: 0
CDP version 2 advertisements output: 50882, Input: 52510
```




Configuring SNMP

This chapter describes how to configure the Simple Network Management Protocol (SNMP) on your access point.



Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges* for this release and to the *Cisco IOS Configuration Fundamentals Command Reference for Release 12.3*.

This chapter consists of these sections:

- [Understanding SNMP, page 17-2](#)
- [Configuring SNMP, page 17-5](#)
- [Configuring SNMP, page 17-5](#)

Understanding SNMP

SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents. The SNMP manager can be part of a network management system (NMS) such as CiscoWorks. The agent and management information base (MIB) reside on the access point. To configure SNMP on the access point, you define the relationship between the manager and the agent.

The SNMP agent contains MIB variables whose values the SNMP manager can request or change. A manager can get a value from an agent or store a value into the agent. The agent gathers data from the MIB, the repository for information about device parameters and network data. The agent can also respond to a manager's requests to get or set data.

An agent can send unsolicited traps to the manager. Traps are messages alerting the SNMP manager to a condition on the network. Traps can mean improper user authentication, restarts, link status (up or down), MAC address tracking, closing of a TCP connection, loss of connection to a neighbor, or other significant events.

This section includes these concepts:

- [SNMP Versions, page 17-2](#)
- [SNMP Manager Functions, page 17-3](#)
- [SNMP Agent Functions, page 17-3](#)
- [SNMP Community Strings, page 17-4](#)
- [Using SNMP to Access MIB Variables, page 17-4](#)

SNMP Versions

This software release supports these SNMP versions:

- SNMPv1—The Simple Network Management Protocol, a full Internet standard, defined in RFC 1157.
- SNMPv2C, which has these features:
 - SNMPv2—Version 2 of the Simple Network Management Protocol, a draft Internet standard, defined in RFCs 1902 through 1907.
 - SNMPv2C—The Community-based Administrative Framework for SNMPv2, an experimental Internet protocol defined in RFC 1901.
- SNMPv3, which has these features:
 - Support for SHA and MD5 authentication protocols and DES56 encryption.
 - Three security levels: no authentication and no privacy (NoAuthNoPriv), authentication and no privacy (AuthNoPriv), and authentication and privacy (AuthPriv).

SNMPv3 supports the highest available levels of security for SNMP communication. Community strings for SNMPv1 and SNMPv2 are stored and transferred as plain text without encryption. In the SNMPv3 security model, SNMP users authenticate and join a user group. Access to system data is restricted based on the group.

You must configure the SNMP agent to use the version of SNMP supported by the management station. An agent can communicate with multiple managers; therefore, you can configure the software to support communications with one management station using the SNMPv3 protocol and another using the SNMPv2 or SNMPv1 protocol.

Table 17-1 lists the SNMP versions and security levels supported on access points:

Table 17-1 SNMP Versions and Security Levels

SNMP Version	Security Level	Authentication	Encryption
v1	NoAuthNoPriv	Community string match	None
v2C	NoAuthNoPriv	Community string match	None
v3	NoAuthNoPriv	Username match	None
v3	AuthNoPriv	HMAC-MD5 or HMAC-SHA algorithms	None
v3	AuthPriv	HMAC-MD5 or HMAC-SHA algorithms	DES 56-bit encryption

For detailed information on SNMPv3, click this link to browse to the *New Feature Documentation* for Cisco IOS Release 12.0(3)T:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t3/snmp3.htm>

SNMP Manager Functions

The SNMP manager uses information in the MIB to perform the operations described in Table 17-2.

Table 17-2 SNMP Operations

Operation	Description
get-request	Retrieves a value from a specific variable.
get-next-request	Retrieves a value from a variable within a table. ¹
get-bulk-request ²	Retrieves large blocks of data that would otherwise require the transmission of many small blocks of data, such as multiple rows in a table.
get-response	Replies to a get-request, get-next-request, and set-request sent by an NMS.
set-request	Stores a value in a specific variable.
trap	An unsolicited message sent by an SNMP agent to an SNMP manager when some event has occurred.

1. With this operation, an SNMP manager does not need to know the exact variable name. A sequential search is performed to find the needed variable from within a table.
2. The **get-bulk** command works only with SNMPv2.

SNMP Agent Functions

The SNMP agent responds to SNMP manager requests as follows:

- Get a MIB variable—The SNMP agent begins this function in response to a request from the NMS. The agent retrieves the value of the requested MIB variable and responds to the NMS with that value.
- Set a MIB variable—The SNMP agent begins this function in response to a message from the NMS. The SNMP agent changes the value of the MIB variable to the value requested by the NMS.

The SNMP agent also sends unsolicited trap messages to notify an NMS that a significant event has occurred on the agent. Examples of trap conditions include, but are not limited to, when a port or module goes up or down, when spanning-tree topology changes occur, and when authentication failures occur.

SNMP Community Strings

SNMP community strings authenticate access to MIB objects and function as embedded passwords. In order for the NMS to access the access point, the community string definitions on the NMS must match at least one of the three community string definitions on the access point.

A community string can have one of these attributes:

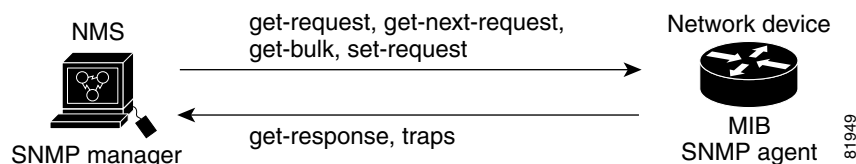
- Read-only—Gives read access to authorized management stations to all objects in the MIB except the community strings, but does not allow write access
- Read-write—Gives read and write access to authorized management stations to all objects in the MIB, but does not allow access to the community strings

Using SNMP to Access MIB Variables

An example of an NMS is the CiscoWorks network management software. CiscoWorks 2000 software uses the access point MIB variables to set device variables and to poll devices on the network for specific information. The results of a poll can be displayed as a graph and analyzed to troubleshoot internetworking problems, increase network performance, verify the configuration of devices, monitor traffic loads, and more.

As shown in [Figure 17-1](#), the SNMP agent gathers data from the MIB. The agent can send traps (notification of certain events) to the SNMP manager, which receives and processes the traps. Traps are messages alerting the SNMP manager to a condition on the network such as improper user authentication, restarts, link status (up or down), MAC address tracking, and so forth. The SNMP agent also responds to MIB-related queries sent by the SNMP manager in *get-request*, *get-next-request*, and *set-request* format.

Figure 17-1 SNMP Network



For information on supported MIBs and how to access them, see [Appendix B, "Supported MIBs."](#)

Configuring SNMP

This section describes how to configure SNMP on your access point. It contains this configuration information:

- [Default SNMP Configuration, page 17-5](#)
- [Enabling the SNMP Agent, page 17-5](#)
- [Configuring Community Strings, page 17-5](#)
- [Configuring Trap Managers and Enabling Traps, page 17-7](#)
- [Setting the Agent Contact and Location Information, page 17-10](#)
- [Using the `snmp-server view` Command, page 17-10](#)
- [SNMP Examples, page 17-10](#)

Default SNMP Configuration

[Table 17-3](#) shows the default SNMP configuration.

Table 17-3 Default SNMP Configuration

Feature	Default Setting
SNMP agent	Disabled
SNMP community strings	No strings are configured by default. However, when you enable SNMP using the web-browser interface, the access point automatically creates the <i>public</i> community with read-only access to the IEEE802dot11 MIB.
SNMP trap receiver	None configured
SNMP traps	None enabled

Enabling the SNMP Agent

No specific CLI command exists to enable SNMP. The first **snmp-server** global configuration command that you enter enables SNMPv1 and SNMPv2.

You can also enable SNMP on the SNMP Properties page on the web-browser interface. When you enable SNMP on the web-browser interface, the access point automatically creates a community string called *public* with read-only access to the IEEE802dot11 MIB.

Configuring Community Strings

You use the SNMP community string to define the relationship between the SNMP manager and the agent. The community string acts like a password to permit access to the agent on the access point.

Optionally, you can specify one or more of these characteristics associated with the string:

- An access list of IP addresses of the SNMP managers that are permitted to use the community string to gain access to the agent

- A MIB view, which defines the subset of all MIB objects accessible to the given community
- Read and write or read-only permission for the MIB objects accessible to the community

**Note**

In the current Cisco IOS MIB agent implementation, the default community string is for the Internet MIB object sub-tree. Because IEEE802dot11 is under another branch of the MIB object tree, you must enable either a separate community string and view on the IEEE802dot11 MIB or a common view and community string on the ISO object in the MIB object tree. ISO is the common parent node of IEEE (IEEE802dot11) and Internet. This MIB agent behavior is different from the MIB agent behavior on access points not running Cisco IOS software.

Beginning in privileged EXEC mode, follow these steps to configure a community string on the access point:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	snmp-server community <i>string</i> [<i>access-list-number</i>] [view <i>mib-view</i>] [ro rw]	Configure the community string. • For <i>string</i>, specify a string that acts like a password and permits access to the SNMP protocol. You can configure one or more community strings of any length. • (Optional) For <i>access-list-number</i>, enter an IP standard access list numbered from 1 to 99 and 1300 to 1999. • (Optional) For view <i>mib-view</i>, specify a MIB view to which this community has access, such as ieee802dot11. See the “Using the snmp-server view Command” section on page 17-10 for instructions on using the snmp-server view command to access Standard IEEE 802.11 MIB objects through IEEE view. • (Optional) Specify either read-only (ro) if you want authorized management stations to retrieve MIB objects, or specify read/write (rw) if you want authorized management stations to retrieve and modify MIB objects. By default, the community string permits read-only access to all objects. Note To access the IEEE802dot11 MIB, you must enable either a separate community string and view on the IEEE802dot11 MIB or a common view and community string on the ISO object in the MIB object tree.

	Command	Purpose
Step 3	access-list <i>access-list-number</i> { deny permit } <i>source</i> [<i>source-wildcard</i>]	(Optional) If you specified an IP standard access list number in Step 2, then create the list, repeating the command as many times as necessary. - For <i>access-list-number</i>, enter the access list number specified in Step 2. - The deny keyword denies access if the conditions are matched. The permit keyword permits access if the conditions are matched. - For <i>source</i>, enter the IP address of the SNMP managers that are permitted to use the community string to gain access to the agent. (Optional) For <i>source-wildcard</i>, enter the wildcard bits in dotted decimal notation to be applied to the source. Place ones in the bit positions that you want to ignore. Recall that the access list is always terminated by an implicit deny statement for everything.
Step 4	end	Return to privileged EXEC mode.
Step 5	show running-config	Verify your entries.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To disable access for an SNMP community, set the community string for that community to the null string (do not enter a value for the community string). To remove a specific community string, use the **no snmp-server community string** global configuration command.

This example shows how to assign the strings *open* and *ieee* to SNMP, to allow read-write access for both, and to specify that *open* is the community string for queries on non-IEEE802dot11-MIB objects and *ieee* is the community string for queries on IEEE802dot11-mib objects:

```
ap(config)# snmp-server view dot11view ieee802dot11 included
ap(config)# snmp-server community open rw
ap(config)# snmp-server community ieee view ieee802dot11 rw
```

Configuring Trap Managers and Enabling Traps

A trap manager is a management station that receives and processes traps. Traps are system alerts that the access point generates when certain events occur. By default, no trap manager is defined, and no traps are issued.

Access points running this Cisco IOS release can have an unlimited number of trap managers. Community strings can be any length.

Table 17-4 describes the supported access point traps (notification types). You can enable any or all of these traps and configure a trap manager to receive them.

Table 17-4 Notification Types

Notification Type	Description
authenticate-fail	Enable traps for authentication failures.
config	Enable traps for SNMP configuration changes.
deauthenticate	Enable traps for client device deauthentications.
disassociate	Enable traps for client device disassociations.
dot11-qos	Enable traps for QoS changes.
entity	Enable traps for SNMP entity changes.
rogue-ap	Enable traps for rogue access point detections.
snmp	Enable traps for SNMP events.
switch-over	Enable traps for switch-overs.
syslog	Enable syslog traps.
wlan-wep	Enable WEP traps.

Some notification types cannot be controlled with the **snmp-server enable** global configuration command, such as **tty** and **udp-port**. These notification types are always enabled. You can use the **snmp-server host** global configuration command to a specific host to receive the notification types listed in [Table 17-4](#).

Beginning in privileged EXEC mode, follow these steps to configure the access point to send traps to a host:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	snmp-server host <i>host-addr</i> { traps informs } { version { 1 2c 3 { auth noauth priv } } } <i>community-string</i> [udp-port <i>port</i>] <i>notification-type</i>	Specify the recipient of the trap message. - For <i>host-addr</i>, specify the name or address of the host (the targeted recipient). - Specify traps (the default) to send SNMP traps to the host. Specify informs to send SNMP informs to the host. - Specify the SNMP version to support. Version 1, the default, is not available with informs. Version 3 has three security levels: auth—Specifies authentication of packets without encryption noauth—Specifies no authentication and no encryption for packets priv—Specifies authentication and encryption for packets - For <i>community-string</i>, specify the string to send with the notification operation. Though you can set this string using the snmp-server host command, Cisco recommends that you define this string by using the snmp-server community command before using the snmp-server host command. - For <i>notification-type</i>, use the keywords listed in Table 17-4 on page 17-8.
Step 3	snmp-server enable traps <i>notification-types</i>	Enable the access point to send specific traps. For a list of traps, see Table 17-4 on page 17-8 . To enable multiple types of traps, you must issue a separate snmp-server enable traps command for each trap type.
Step 4	end	Return to privileged EXEC mode.
Step 5	show running-config	Verify your entries.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To remove the specified host from receiving traps, use the **no snmp-server host** *host* global configuration command. To disable a specific trap type, use the **no snmp-server enable traps** *notification-types* global configuration command.

Setting the Agent Contact and Location Information

Beginning in privileged EXEC mode, follow these steps to set the system contact and location of the SNMP agent so that these descriptions can be accessed through the configuration file:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	snmp-server contact <i>text</i>	Set the system contact string. For example: snmp-server contact Dial System Operator at beeper 21555.
Step 3	snmp-server location <i>text</i>	Set the system location string. For example: snmp-server location Building 3/Room 222
Step 4	end	Return to privileged EXEC mode.
Step 5	show running-config	Verify your entries.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Using the snmp-server view Command

In global configuration mode, use the **snmp-server view** command to access Standard IEEE 802.11 MIB objects through IEEE view and the dot11 read-write community string.

This example shows how to enable IEEE view and dot11 read-write community string:

```
ap(config)# snmp-server view ieee ieee802dot11 included
ap(config)# snmp-server community dot11 view ieee RW
```

SNMP Examples

This example shows how to enable SNMPv1 and SNMPv2C. The configuration permits any SNMP manager to access all objects with read-only permissions using the community string *public*. This configuration does not cause the access point to send any traps.

```
AP(config)# snmp-server community public
```

This example shows how to assign the strings *open* and *ieee* to SNMP, to allow read-write access for both, and to specify that *open* is the community string for queries on non-IEEE802dot11-MIB objects and *ieee* is the community string for queries on IEEE802dot11-mib objects:

```
ap(config)# snmp-server view dot11view ieee802dot11 included
ap(config)# snmp-server community open rw
ap(config)# snmp-server community ieee view ieee802dot11 rw
```


This example shows how to permit any SNMP manager to access all objects with read-only permission using the community string *public*. The access point also sends config traps to the hosts 192.180.1.111 and 192.180.1.33 using SNMPv1 and to the host 192.180.1.27 using SNMPv2C. The community string *public* is sent with the traps.

```
ap(config)# snmp-server community public
ap(config)# snmp-server enable traps config
ap(config)# snmp-server host 192.180.1.27 version 2c public
ap(config)# snmp-server host 192.180.1.111 version 1 public
ap(config)# snmp-server host 192.180.1.33 public
```

This example shows how to allow read-only access for all objects to members of access list 4 that use the *comaccess* community string. No other SNMP managers have access to any objects. SNMP Authentication Failure traps are sent by SNMPv2C to the host *cisco.com* using the community string *public*.

```
ap(config)# snmp-server community comaccess ro 4
ap(config)# snmp-server enable traps snmp authentication
ap(config)# snmp-server host cisco.com version 2c public
```

This example shows how to send Entity MIB traps to the host *cisco.com*. The community string is restricted. The first line enables the access point to send Entity MIB traps in addition to any traps previously enabled. The second line specifies the destination of these traps and overwrites any previous **snmp-server host** commands for the host *cisco.com*.

```
ap(config)# snmp-server enable traps entity
ap(config)# snmp-server host cisco.com restricted entity
```

This example shows how to enable the access point to send all traps to the host *myhost.cisco.com* using the community string *public*:

```
ap(config)# snmp-server enable traps
ap(config)# snmp-server host myhost.cisco.com public
```

Displaying SNMP Status

To display SNMP input and output statistics, including the number of illegal community string entries, errors, and requested variables, use the **show snmp** privileged EXEC command. For information about the fields in this display, refer to the *Cisco IOS Configuration Fundamentals Command Reference for Release 12.3*.



Managing Firmware and Configurations

This chapter describes how to manipulate the Flash file system, how to copy configuration files, and how to archive (upload and download) software images.



Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges* for this release and the *Cisco IOS Configuration Fundamentals Command Reference for Release 12.3*.

This chapter consists of these sections:

- [Working with the Flash File System, page 18-2](#)
- [Working with Configuration Files, page 18-8](#)
- [Working with Software Images, page 18-19](#)

Working with the Flash File System

The Flash file system on your access point/bridge provides several commands to help you manage software image and configuration files.

The Flash file system is a single Flash device on which you can store files. This Flash device is called *flash:*.

This section contains this information:

- [Displaying Available File Systems, page 18-2](#)
- [Setting the Default File System, page 18-3](#)
- [Displaying Information About Files on a File System, page 18-3](#)
- [Changing Directories and Displaying the Working Directory, page 18-4](#)
- [Creating and Removing Directories, page 18-4](#)
- [Copying Files, page 18-5](#)
- [Deleting Files, page 18-5](#)
- [Creating, Displaying, and Extracting tar Files, page 18-6](#)
- [Displaying the Contents of a File, page 18-8](#)

Displaying Available File Systems

To display the available file systems on your access point/bridge, use the **show file systems** privileged EXEC command as shown in this example:

```
ap# show file systems
File Systems:

      Size(b)      Free(b)      Type  Flags  Prefixes
*  16128000      11118592      flash   rw    flash:
  16128000      11118592      unknown rw    zflash:
      32768        26363      nvram   rw    nvram:
      -           -      network rw    tftp:
      -           -      opaque  rw    null:
      -           -      opaque  rw    system:
      -           -      opaque  ro    xmodem:
      -           -      opaque  ro    ymodem:
      -           -      network rw    rcpx:
      -           -      network rw    ftp:
```

[Table 18-1](#) lists field descriptions for the **show file systems** command.

Table 18-1 *show file systems Field Descriptions*

Field	Value
Size(b)	Amount of memory in the file system in bytes.
Free(b)	Amount of free memory in the file system in bytes.

Table 18-1 show file systems Field Descriptions (continued)

Field	Value
Type	Type of file system. flash —The file system is for a Flash memory device. network —The file system is for a network device. nvr am—The file system is for a nonvolatile RAM (NVRAM) device. opaque —The file system is a locally generated <i>pseudo</i> file system (for example, the <i>system</i>) or a download interface, such as brimux. unknown —The file system is an unknown type.
Flags	Permission for file system. ro —read-only. rw —read/write. wo —write-only.
Prefixes	Alias for file system. flash: —Flash file system. ftp: —File Transfer Protocol network server. Used to transfer files to or from the network device. nvr am:—Non-volatile RAM memory (NVRAM). null: —Null destination for copies. You can copy a remote file to null to determine its size. r cp:—Remote Copy Protocol (RCP) network server. s ystem:—Contains the system memory, including the running configuration. t ftp:—Trivial File Transfer Protocol (TFTP) network server. z flash:—Read-only file decompression file system, which mirrors the contents of the Flash file system.

Setting the Default File System

You can specify the file system or directory that the system uses as the default file system by using the **cd filesystem:** privileged EXEC command. You can set the default file system to omit the *filesystem:* argument from related commands. For example, for all privileged EXEC commands that have the optional *filesystem:* argument, the system uses the file system specified by the **cd** command.

By default, the default file system is *flash:*.

You can display the current default file system as specified by the **cd** command by using the **pwd** privileged EXEC command.

Displaying Information About Files on a File System

You can view a list of the contents of a file system before manipulating its contents. For example, before copying a new configuration file to Flash memory, you might want to verify that the file system does not already contain a configuration file with the same name. Similarly, before copying a Flash configuration file to another location, you might want to verify its filename for use in another command.

To display information about files on a file system, use one of the privileged EXEC commands in [Table 18-2](#):

Table 18-2 Commands for Displaying Information About Files

Command	Description
dir [/all] [filesystem:][filename]	Display a list of files on a file system.
show file systems	Display more information about each of the files on a file system.
show file information file-url	Display information about a specific file.
show file descriptors	Display a list of open file descriptors. File descriptors are the internal representations of open files. You can use this command to see if another user has a file open.

Changing Directories and Displaying the Working Directory

Beginning in privileged EXEC mode, follow these steps to change directories and display the working directory.

	Command	Purpose
Step 1	dir filesystem:	Display the directories on the specified file system. For <i>filesystem:</i> , use flash: for the system board Flash device.
Step 2	cd new_configs	Change to the directory of interest. The command example shows how to change to the directory named <i>new_configs</i> .
Step 3	pwd	Display the working directory.

Creating and Removing Directories

Beginning in privileged EXEC mode, follow these steps to create and remove a directory:

	Command	Purpose
Step 1	dir filesystem:	Display the directories on the specified file system. For <i>filesystem:</i> , use flash: for the system board Flash device.
Step 2	mkdir old_configs	Create a new directory. The command example shows how to create the directory named <i>old_configs</i> . Directory names are case sensitive. Directory names are limited to 45 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.
Step 3	dir filesystem:	Verify your entry.

To delete a directory with all its files and subdirectories, use the **delete /force /recursive** *filesystem:/file-url* privileged EXEC command.

Use the **/recursive** keyword to delete the named directory and all subdirectories and the files contained in it. Use the **/force** keyword to suppress the prompting that confirms a deletion of each file in the directory. You are prompted only once at the beginning of this deletion process. Use the **/force** and **/recursive** keywords for deleting old software images that were installed by using the **archive download-sw** command but are no longer needed.

For *filesystem*, use **flash:** for the system board Flash device. For *file-url*, enter the name of the directory to be deleted. All the files in the directory and the directory are removed.

**Caution**

When files and directories are deleted, their contents cannot be recovered.

Copying Files

To copy a file from a source to a destination, use the **copy** [**/erase**] *source-url destination-url* privileged EXEC command. For the source and destination URLs, you can use **running-config** and **startup-config** keyword shortcuts. For example, the **copy running-config startup-config** command saves the currently running configuration file to the NVRAM section of Flash memory to be used as the configuration during system initialization.

Network file system URLs include **ftp:**, **rcp:**, and **tftp:** and have the following syntax:

- File Transfer Protocol (FTP)—**ftp:**[[*//username* [*:password*]]@*location*]/*directory*]/*filename*
- Remote Copy Protocol (RCP)—**rcp:**[[*//username*@*location*]/*directory*]/*filename*
- Trivial File Transfer Protocol (TFTP)—**tftp:**[[*//location*]/*directory*]/*filename*

Local writable file systems include flash:

Some invalid combinations of source and destination exist. Specifically, you cannot copy these combinations:

- From a running configuration to a running configuration
- From a startup configuration to a startup configuration
- From a device to the same device (for example, the **copy flash: flash:** command is invalid)

For specific examples of using the **copy** command with configuration files, see the [“Working with Configuration Files” section on page 18-8](#).

To copy software images either by downloading a new version or uploading the existing one, use the **archive download-sw** or the **archive upload-sw** privileged EXEC command. For more information, see the [“Working with Software Images” section on page 18-19](#).

Deleting Files

When you no longer need a file on a Flash memory device, you can permanently delete it. To delete a file or directory from a specified Flash device, use the **delete** [**/force**] [**/recursive**] [*filesystem:*]/*file-url* privileged EXEC command.

**Caution**

When files are deleted, their contents cannot be recovered.

Use the **/recursive** keyword for deleting a directory and all subdirectories and the files contained in it. Use the **/force** keyword to suppress the prompting that confirms a deletion of each file in the directory. You are prompted only once at the beginning of this deletion process. Use the **/force** and **/recursive** keywords for deleting old software images that were installed by using the **archive download-sw** command but are no longer needed.

If you omit the *filesystem:* option, the access point/bridge uses the default device specified by the **cd** command. For *file-url*, you specify the path (directory) and the name of the file to be deleted.

This example shows how to delete the file *myconfig* from the default Flash memory device:

```
ap# delete myconfig
```

Creating, Displaying, and Extracting tar Files

You can create a tar file and write files into it, list the files in a tar file, and extract the files from a tar file as described in the next sections.

Creating a tar File

To create a tar file and write files into it, use this privileged EXEC command:

```
archive tar /create destination-url flash:/file-url
```

For *destination-url*, specify the destination URL alias for the local or network file system and the name of the tar file to create. These options are supported:

- For the local Flash file system, the syntax is **flash:/file-url**
- For the File Transfer Protocol (FTP), the syntax is **ftp:[[/username[:password]@location]/directory]/tar-filename.tar**
- For the Remote Copy Protocol (RCP), the syntax is **rcp:[[/username@location]/directory]/tar-filename.tar**
- For the Trivial File Transfer Protocol (TFTP), the syntax is **tftp:[[/location]/directory]/tar-filename.tar**

The *tar-filename.tar* is the tar file to be created.

For **flash:/file-url**, specify the location on the local Flash file system from which the new tar file is created. You can also specify an optional list of files or directories within the source directory to write to the new tar file. If none are specified, all files and directories at this level are written to the newly created tar file.

This example shows how to create a tar file. This command writes the contents of the *new-configs* directory on the local Flash device to a file named *saved.tar* on the TFTP server at 172.20.10.30:

```
ap# archive tar /create tftp:172.20.10.30/saved.tar flash:/new-configs
```


Displaying the Contents of a tar File

To display the contents of a tar file on the screen, use this privileged EXEC command:

archive tar /table *source-url*

For *source-url*, specify the source URL alias for the local or network file system. These options are supported:

- For the local Flash file system, the syntax is **flash:**
- For the File Transfer Protocol (FTP), the syntax is **ftp:[[/username[:password]@location]/directory]/tar-filename.tar**
- For the Remote Copy Protocol (RCP), the syntax is **rnp:[[/username@location]/directory]/tar-filename.tar**
- For the Trivial File Transfer Protocol (TFTP), the syntax is **tftp:[[/location]/directory]/tar-filename.tar**

The *tar-filename.tar* is the tar file to display.

You can also limit the display of the files by specifying an optional list of files or directories after the tar file; then only these files are displayed. If none are specified, all files and directories are displayed.

This example shows how to display the contents of the *c1200-k9w7-mx.122-8.JA.tar* file that is in Flash memory:

```
ap# archive tar /table flash:c1200-k9w7-mx.122-8.JA.tar
info (219 bytes)
c1200-k9w7-mx.122-11.JA/ (directory)
c1200-k9w7-mx.122-11.JA/html/ (directory)
c1200-k9w7-mx.122-11.JA/html/foo.html (0 bytes)
c1200-k9w7-mx.122-11.JA/c1200-k9w7-mx.122-8.JA.bin (610856 bytes)
c1200-k9w7-mx.122-11.JA/info (219 bytes)
info.ver (219 bytes)
```

This example shows how to display only the *c1200-k9w7-mx.122-8.JA/html* directory and its contents:

```
ap# archive tar /table flash:c1200-k9w7-mx.122-8.JA/html
c1200-k9w7-mx.122-11.JA/html/ (directory)
c1200-k9w7-mx.122-11.JA/html/foo.html (0 bytes)
```

Extracting a tar File

To extract a tar file into a directory on the Flash file system, use this privileged EXEC command:

archive tar /xtract *source-url* **flash:/file-url**

For *source-url*, specify the source URL alias for the local or network file system. These options are supported:

- For the local Flash file system, the syntax is **flash:**
- For the File Transfer Protocol (FTP), the syntax is **ftp:[[/username[:password]@location]/directory]/tar-filename.tar**
- For the Remote Copy Protocol (RCP), the syntax is **rnp:[[/username@location]/directory]/tar-filename.tar**
- For the Trivial File Transfer Protocol (TFTP), the syntax is **tftp:[[/location]/directory]/tar-filename.tar**

The *tar-filename.tar* is the tar file from which to extract files.

For **flash:/file-url**, specify the location on the local Flash file system into which the tar file is extracted. You can also specify an optional list of files or directories within the tar file for extraction. If none are specified, all files and directories are extracted.

This example shows how to extract the contents of a tar file located on the TFTP server at 172.20.10.30. This command extracts just the *new-configs* directory into the root directory on the local Flash file system. The remaining files in the *saved.tar* file are ignored.

```
ap# archive tar /xtract tftp://172.20.10.30/saved.tar flash:/new-configs
```

Displaying the Contents of a File

To display the contents of any readable file, including a file on a remote file system, use the **more** [/ascii | /binary | /ebcdic] *file-url* privileged EXEC command:

This example shows how to display the contents of a configuration file on a TFTP server:

```
ap# more tftp://serverA/hampton/savedconfig
!
! Saved configuration on server
!
version 11.3
service timestamps log datetime localtime
service linenummer
service udp-small-servers
service pt-vty-logging
!

<output truncated>
```

Working with Configuration Files

This section describes how to create, load, and maintain configuration files. Configuration files contain commands entered to customize the function of the Cisco IOS software. To better benefit from these instructions, your access point/bridge contains a minimal default running configuration for interacting with the system software.

You can copy (*download*) configuration files from a TFTP, FTP, or RCP server to the running configuration of the access point/bridge for various reasons:

- To restore a backed-up configuration file.
- To use the configuration file for another access point/bridge. For example, you might add another access point/bridge to your network and want it to have a configuration similar to the original access point/bridge. By copying the file to the new access point/bridge, you can change the relevant parts rather than recreating the whole file.
- To load the same configuration commands on all the access points in your network so that all the access points have similar configurations.

You can copy (*upload*) configuration files from the access point/bridge to a file server by using TFTP, FTP, or RCP. You might perform this task to back up a current configuration file to a server before changing its contents so that you can later restore the original configuration file from the server.

The protocol you use depends on which type of server you are using. The FTP and RCP transport mechanisms provide faster performance and more reliable delivery of data than TFTP. These improvements are possible because FTP and RCP are built on and use the Transmission Control Protocol/Internet Protocol (TCP/IP) stack, which is connection oriented.

This section includes this information:

- [Guidelines for Creating and Using Configuration Files, page 18-9](#)
- [Configuration File Types and Location, page 18-10](#)
- [Creating a Configuration File by Using a Text Editor, page 18-10](#)
- [Copying Configuration Files by Using TFTP, page 18-10](#)
- [Copying Configuration Files by Using FTP, page 18-12](#)
- [Copying Configuration Files by Using RCP, page 18-15](#)
- [Clearing Configuration Information, page 18-18](#)

Guidelines for Creating and Using Configuration Files

Creating configuration files can aid in your access point/bridge configuration. Configuration files can contain some or all of the commands needed to configure one or more access points. For example, you might want to download the same configuration file to several access points that have the same hardware configuration.

Use these guidelines when creating a configuration file:

- If no passwords have been set on the access point/bridge, you must set them on each access point/bridge by entering the **enable secret** *secret-password* global configuration command. Enter a blank line for this command. The password is saved in the configuration file as clear text.
- If passwords already exist, you cannot enter the **enable secret** *secret-password* global configuration command in the file because the password verification will fail. If you enter a password in the configuration file, the access point/bridge mistakenly attempts to execute the passwords as commands as it executes the file.
- The **copy {ftp: | rcp: | tftp:} system:running-config** privileged EXEC command loads the configuration files on the access point/bridge as if you were entering the commands at the command line. The access point/bridge does not erase the existing running configuration before adding the commands. If a command in the copied configuration file replaces a command in the existing configuration file, the existing command is erased. For example, if the copied configuration file contains a different IP address in a particular command than the existing configuration, the IP address in the copied configuration is used. However, some commands in the existing configuration might not be replaced or negated. In this case, the resulting configuration file is a mixture of the existing configuration file and the copied configuration file, with the copied configuration file having precedence.

To restore a configuration file to an exact copy of a file stored on a server, copy the configuration file directly to the startup configuration (by using the **copy {ftp: | rcp: | tftp:} nvram:startup-config** privileged EXEC command), and reload the access point/bridge.

Configuration File Types and Location

Startup configuration files are used during system startup to configure the software. Running configuration files contain the current configuration of the software. The two configuration files can be different. For example, you might want to change the configuration for a short time period rather than permanently. In this case, you would change the running configuration but not save the configuration by using the **copy running-config startup-config** privileged EXEC command.

The running configuration is saved in DRAM; the startup configuration is stored in the NVRAM section of Flash memory.

Creating a Configuration File by Using a Text Editor

When creating a configuration file, you must list commands logically so that the system can respond appropriately. This is one method of creating a configuration file:

-
Step 1	Copy an existing configuration from an access point/bridge to a server. For more information, see the “Downloading the Configuration File by Using TFTP” section on page 18-11, the “Downloading a Configuration File by Using FTP” section on page 18-13, or the “Downloading a Configuration File by Using RCP” section on page 18-17.
Step 2	Open the configuration file in a text editor such as vi or emacs on UNIX or Notepad on a PC.
Step 3	Extract the portion of the configuration file with the desired commands, and save it in a new file.
Step 4	Copy the configuration file to the appropriate server location. For example, copy the file to the TFTP directory on the workstation (usually /tftpboot on a UNIX workstation).
Step 5	Make sure the permissions on the file are set to world-read.
-

Copying Configuration Files by Using TFTP

You can configure the access point/bridge by using configuration files you create, download from another access point/bridge, or download from a TFTP server. You can copy (upload) configuration files to a TFTP server for storage.

This section includes this information:

- [Preparing to Download or Upload a Configuration File by Using TFTP, page 18-10](#)
- [Downloading the Configuration File by Using TFTP, page 18-11](#)
- [Uploading the Configuration File by Using TFTP, page 18-12](#)

Preparing to Download or Upload a Configuration File by Using TFTP

Before you begin downloading or uploading a configuration file by using TFTP, perform these tasks:

- Ensure that the workstation acting as the TFTP server is properly configured. On a Sun workstation, make sure that the /etc/inetd.conf file contains this line:

```
tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd -p -s /tftpboot
```

Make sure that the `/etc/services` file contains this line:

```
tftp 69/udp
```



Note You must restart the `inetd` daemon after modifying the `/etc/inetd.conf` and `/etc/services` files. To restart the daemon, either stop the `inetd` process and restart it, or enter a **fastboot** command (on the SunOS 4.x) or a **reboot** command (on Solaris 2.x or SunOS 5.x). For more information on the TFTP daemon, refer to the documentation for your workstation.

- Ensure that the access point/bridge has a route to the TFTP server. The access point/bridge and the TFTP server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the TFTP server by using the **ping** command.
- Ensure that the configuration file to be downloaded is in the correct directory on the TFTP server (usually `/tftpboot` on a UNIX workstation).
- For download operations, ensure that the permissions on the file are set correctly. The permission on the file should be world-read.
- Before uploading the configuration file, you might need to create an empty file on the TFTP server. To create an empty file, enter the **touch filename** command, where *filename* is the name of the file you will use when uploading it to the server.
- During upload operations, if you are overwriting an existing file (including an empty file, if you had to create one) on the server, ensure that the permissions on the file are set correctly. Permissions on the file should be world-write.

Downloading the Configuration File by Using TFTP

To configure the access point/bridge by using a configuration file downloaded from a TFTP server, follow these steps:

-
- Step 1** Copy the configuration file to the appropriate TFTP directory on the workstation.
- Step 2** Verify that the TFTP server is properly configured by referring to the [“Preparing to Download or Upload a Configuration File by Using TFTP”](#) section on page 18-10.
- Step 3** Log into the access point/bridge through a Telnet session.
- Step 4** Download the configuration file from the TFTP server to configure the access point/bridge. Specify the IP address or host name of the TFTP server and the name of the file to download. Use one of these privileged EXEC commands:
- **copy tftp:[*[[location]/directory]/filename*] system:running-config**
 - **copy tftp:[*[[location]/directory]/filename*] nvram:startup-config**
- The configuration file downloads, and the commands are executed as the file is parsed line-by-line.
-

This example shows how to configure the software from the file *tokyo-config* at IP address 172.16.2.155:

```
ap# copy tftp://172.16.2.155/tokyo-config system:running-config
Configure using tokyo-config from 172.16.2.155? [confirm] y
Booting tokyo-config from 172.16.2.155:!!! [OK - 874/16000 bytes]
```

Uploading the Configuration File by Using TFTP

To upload a configuration file from an access point/bridge to a TFTP server for storage, follow these steps:

-
- Step 1** Verify that the TFTP server is properly configured by referring to the “[Preparing to Download or Upload a Configuration File by Using TFTP](#)” section on page 18-10.
- Step 2** Log into the access point/bridge through a Telnet session.
- Step 3** Upload the access point/bridge configuration to the TFTP server. Specify the IP address or host name of the TFTP server and the destination filename.

Use one of these privileged EXEC commands:

- **copy system:running-config tftp:**[[*location*]/*directory*]/*filename*]
- **copy nvram:startup-config tftp:**[[*location*]/*directory*]/*filename*]

The file is uploaded to the TFTP server.

This example shows how to upload a configuration file from an access point/bridge to a TFTP server:

```
ap# copy system:running-config tftp://172.16.2.155/tokyo-config
Write file tokyo-config on host 172.16.2.155? [confirm] y
#
Writing tokyo-config!!! [OK]
```

Copying Configuration Files by Using FTP

You can copy configuration files to or from an FTP server.

The FTP protocol requires a client to send a remote username and password on each FTP request to a server. When you copy a configuration file from the access point/bridge to a server by using FTP, the Cisco IOS software sends the first valid username in this list:

- The username specified in the **copy** command if a username is specified.
- The username set by the **ip ftp username** *username* global configuration command if the command is configured.
- Anonymous.

The access point/bridge sends the first valid password in this list:

- The password specified in the **copy** command if a password is specified.
- The password set by the **ip ftp password** *password* global configuration command if the command is configured.
- The access point/bridge forms a password named *username@apname.domain*. The variable *username* is the username associated with the current session, *apname* is the configured host name, and *domain* is the domain of the access point/bridge.

The username and password must be associated with an account on the FTP server. If you are writing to the server, the FTP server must be properly configured to accept your FTP write request.

Use the **ip ftp username** and **ip ftp password** commands to specify a username and password for all copies. Include the username in the **copy** command if you want to specify only a username for that copy operation.

If the server has a directory structure, the configuration file is written to or copied from the directory associated with the username on the server. For example, if the configuration file resides in the home directory of a user on the server, specify that user's name as the remote username.

For more information, refer to the documentation for your FTP server.

This section includes this information:

- [Preparing to Download or Upload a Configuration File by Using FTP, page 18-13](#)
- [Downloading a Configuration File by Using FTP, page 18-13](#)
- [Uploading a Configuration File by Using FTP, page 18-14](#)

Preparing to Download or Upload a Configuration File by Using FTP

Before you begin downloading or uploading a configuration file by using FTP, perform these tasks:

- Ensure that the access point/bridge has a route to the FTP server. The access point/bridge and the FTP server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the FTP server by using the **ping** command.
- If you are accessing the access point/bridge through a Telnet session and you do not have a valid username, make sure that the current FTP username is the one that you want to use for the FTP download. You can enter the **show users** privileged EXEC command to view the valid username. If you do not want to use this username, create a new FTP username by using the **ip ftp username *username*** global configuration command during all copy operations. The new username is stored in NVRAM. If you are accessing the access point/bridge through a Telnet session and you have a valid username, this username is used, and you do not need to set the FTP username. Include the username in the **copy** command if you want to specify a username for only that copy operation.
- When you upload a configuration file to the FTP server, it must be properly configured to accept the write request from the user on the access point/bridge.

For more information, refer to the documentation for your FTP server.

Downloading a Configuration File by Using FTP

Beginning in privileged EXEC mode, follow these steps to download a configuration file by using FTP:

	Command	Purpose
Step 1		Verify that the FTP server is properly configured by referring to the “Preparing to Download or Upload a Configuration File by Using FTP” section on page 18-13.
Step 2		Log into the access point/bridge through a Telnet session.
Step 3	configure terminal	Enter global configuration mode on the access point/bridge. This step is required only if you override the default remote username or password (see Steps 4, 5, and 6).
Step 4	ip ftp username <i>username</i>	(Optional) Change the default remote username.
Step 5	ip ftp password <i>password</i>	(Optional) Change the default password.

	Command	Purpose
Step 6	end	Return to privileged EXEC mode.
Step 7	copy ftp:[username[:password]@]location[/directory] /filename] system:running-config or copy ftp:[username[:password]@]location[/directory] /filename] nvram:startup-config	Using FTP, copy the configuration file from a network server to the running configuration or to the startup configuration file.

This example shows how to copy a configuration file named *host1-config* from the *netadmin1* directory on the remote server with an IP address of 172.16.101.101 and to load and run those commands on the access point/bridge:

```
ap# copy ftp://netadmin1:mypass@172.16.101.101/host1-config system:running-config
Configure using host1-config from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-config:![OK]
ap#
%SYS-5-CONFIG: Configured from host1-config by ftp from 172.16.101.101
```

This example shows how to specify a remote username of *netadmin1*. The software copies the configuration file *host2-config* from the *netadmin1* directory on the remote server with an IP address of 172.16.101.101 to the access point/bridge startup configuration.

```
ap# configure terminal
ap(config)# ip ftp username netadmin1
ap(config)# ip ftp password mypass
ap(config)# end
ap# copy ftp: nvram:startup-config
Address of remote host [255.255.255.255]? 172.16.101.101
Name of configuration file[rtr2-config]? host2-config
Configure using host2-config from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-config:![OK]
[OK]
ap#
%SYS-5-CONFIG_NV:Non-volatile store configured from host2-config by ftp from
172.16.101.101
```

Uploading a Configuration File by Using FTP

Beginning in privileged EXEC mode, follow these steps to upload a configuration file by using FTP:

	Command	Purpose
Step 1		Verify that the FTP server is properly configured by referring to the “Preparing to Download or Upload a Configuration File by Using FTP” section on page 18-13.
Step 2		Log into the access point/bridge through a Telnet session.
Step 3	configure terminal	Enter global configuration mode. This step is required only if you override the default remote username or password (see Steps 4, 5, and 6).

	Command	Purpose
Step 4	ip ftp username <i>username</i>	(Optional) Change the default remote username.
Step 5	ip ftp password <i>password</i>	(Optional) Change the default password.
Step 6	end	Return to privileged EXEC mode.
Step 7	copy system:running-config ftp:[[/[username[:password]@]location]/directory] <i>/filename]</i> or copy nvram:startup-config ftp:[[/[username[:password]@]location]/directory] <i>/filename]</i>	Using FTP, store the access point/bridge running or startup configuration file to the specified location.

This example shows how to copy the running configuration file named *ap2-confg* to the *netadmin1* directory on the remote host with an IP address of 172.16.101.101:

```
ap# copy system:running-config ftp://netadmin1:mypass@172.16.101.101/ap2-confg
Write file ap2-confg on host 172.16.101.101?[confirm]
Building configuration...[OK]
Connected to 172.16.101.101
ap#
```

This example shows how to store a startup configuration file on a server by using FTP to copy the file:

```
ap# configure terminal
ap(config)# ip ftp username netadmin2
ap(config)# ip ftp password mypass
ap(config)# end
ap# copy nvram:startup-config ftp:
Remote host[]? 172.16.101.101
Name of configuration file to write [ap2-confg]?
Write file ap2-confg on host 172.16.101.101?[confirm]
![OK]
```

Copying Configuration Files by Using RCP

The Remote Copy Protocol (RCP) provides another method of downloading, uploading, and copying configuration files between remote hosts and the access point/bridge. Unlike TFTP, which uses User Datagram Protocol (UDP), a connectionless protocol, RCP uses TCP, which is connection-oriented.

To use RCP to copy files, the server from or to which you will be copying files must support RCP. The RCP copy commands rely on the rsh server (or daemon) on the remote system. To copy files by using RCP, you do not need to create a server for file distribution as you do with TFTP. You only need to have access to a server that supports the remote shell (rsh). (Most UNIX systems support rsh.) Because you are copying a file from one place to another, you must have read permission on the source file and write permission on the destination file. If the destination file does not exist, RCP creates it for you.

The RCP requires a client to send a remote username with each RCP request to a server. When you copy a configuration file from the access point/bridge to a server, the Cisco IOS software sends the first valid username in this list:

- The username specified in the **copy** command if a username is specified.
- The username set by the **ip rcmd remote-username** *username* global configuration command if the command is configured.

- The remote username associated with the current TTY (terminal) process. For example, if the user is connected to the router through Telnet and was authenticated through the **username** command, the access point/bridge software sends the Telnet username as the remote username.
- The access point/bridge host name.

For a successful RCP copy request, you must define an account on the network server for the remote username. If the server has a directory structure, the configuration file is written to or copied from the directory associated with the remote username on the server. For example, if the configuration file is in the home directory of a user on the server, specify that user's name as the remote username.

This section includes this information:

- [Preparing to Download or Upload a Configuration File by Using RCP, page 18-16](#)
- [Downloading a Configuration File by Using RCP, page 18-17](#)
- [Uploading a Configuration File by Using RCP, page 18-18](#)

Preparing to Download or Upload a Configuration File by Using RCP

Before you begin downloading or uploading a configuration file by using RCP, perform these tasks:

- Ensure that the workstation acting as the RCP server supports the remote shell (rsh).
- Ensure that the access point/bridge has a route to the RCP server. The access point/bridge and the server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the RCP server by using the **ping** command.
- If you are accessing the access point/bridge through a Telnet session and you do not have a valid username, make sure that the current RCP username is the one that you want to use for the RCP download. You can enter the **show users** privileged EXEC command to view the valid username. If you do not want to use this username, create a new RCP username by using the **ip rcmd remote-username username** global configuration command to be used during all copy operations. The new username is stored in NVRAM. If you are accessing the access point/bridge through a Telnet session and you have a valid username, this username is used, and you do not need to set the RCP username. Include the username in the **copy** command if you want to specify a username for only that copy operation.
- When you upload a file to the RCP server, it must be properly configured to accept the RCP write request from the user on the access point/bridge. For UNIX systems, you must add an entry to the **.rhosts** file for the remote user on the RCP server. For example, suppose that the access point/bridge contains these configuration lines:

```
hostname ap1
ip rcmd remote-username User0
```

If the access point/bridge IP address translates to *ap1.company.com*, the **.rhosts** file for User0 on the RCP server should contain this line:

```
ap1.company.com ap1
```

For more information, refer to the documentation for your RCP server.

Downloading a Configuration File by Using RCP

Beginning in privileged EXEC mode, follow these steps to download a configuration file by using RCP:

	Command	Purpose
Step 1		Verify that the RCP server is properly configured by referring to the “Preparing to Download or Upload a Configuration File by Using RCP” section on page 18-16.
Step 2		Log into the access point/bridge through a Telnet session.
Step 3	configure terminal	Enter global configuration mode. This step is required only if you override the default remote username (see Steps 4 and 5).
Step 4	ip rcmd remote-username <i>username</i>	(Optional) Specify the remote username.
Step 5	end	Return to privileged EXEC mode.
Step 6	copy rcp:[[/[<i>username@</i>]<i>location</i>]/<i>directory</i>]/<i>filename</i>] system:running-config or copy rcp:[[/[<i>username@</i>]<i>location</i>]/<i>directory</i>]/<i>filename</i>] nvrn:startup-config	Using RCP, copy the configuration file from a network server to the running configuration or to the startup configuration file.

This example shows how to copy a configuration file named *host1-config* from the *netadmin1* directory on the remote server with an IP address of 172.16.101.101 and load and run those commands on the access point/bridge:

```
ap# copy rcp://netadmin1@172.16.101.101/host1-config system:running-config
Configure using host1-config from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-config:[OK]
ap#
%SYS-5-CONFIG: Configured from host1-config by rcp from 172.16.101.101
```

This example shows how to specify a remote username of *netadmin1*. Then it copies the configuration file *host2-config* from the *netadmin1* directory on the remote server with an IP address of 172.16.101.101 to the startup configuration:

```
ap# configure terminal
ap(config)# ip rcmd remote-username netadmin1
ap(config)# end
ap# copy rcp: nvrn:startup-config
Address of remote host [255.255.255.255]? 172.16.101.101
Name of configuration file[rtr2-config]? host2-config
Configure using host2-config from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-config:[OK]
[OK]
ap#
%SYS-5-CONFIG_NV:Non-volatile store configured from host2-config by rcp from
172.16.101.101
```

Uploading a Configuration File by Using RCP

Beginning in privileged EXEC mode, follow these steps to upload a configuration file by using RCP:

	Command	Purpose
Step 1		Verify that the RCP server is properly configured by referring to the “Preparing to Download or Upload a Configuration File by Using RCP” section on page 18-16.
Step 2		Log into the access point/bridge through a Telnet session.
Step 3	configure terminal	Enter global configuration mode. This step is required only if you override the default remote username (see Steps 4 and 5).
Step 4	ip rcmd remote-username <i>username</i>	(Optional) Specify the remote username.
Step 5	end	Return to privileged EXEC mode.
Step 6	copy system:running-config rcp:[[/[username@]location]/directory]/filename] or copy nvram:startup-config rcp:[[/[username@]location]/directory]/filename]	Using RCP, copy the configuration file from an access point/bridge running or startup configuration file to a network server.

This example shows how to copy the running configuration file named *ap2-confg* to the *netadmin1* directory on the remote host with an IP address of 172.16.101.101:

```
ap# copy system:running-config rcp://netadmin1@172.16.101.101/ap2-confg
Write file br-confg on host 172.16.101.101?[confirm]
Building configuration...[OK]
Connected to 172.16.101.101
ap#
```

This example shows how to store a startup configuration file on a server:

```
ap# configure terminal
ap(config)# ip rcmd remote-username netadmin2
ap(config)# end
ap# copy nvram:startup-config rcp:
Remote host[]? 172.16.101.101
Name of configuration file to write [ap2-confg]?
Write file ap2-confg on host 172.16.101.101?[confirm]
![OK]
```

Clearing Configuration Information

This section describes how to clear configuration information.

Deleting a Stored Configuration File



Caution

You cannot restore a file after it has been deleted.

To delete a saved configuration from Flash memory, use the **delete flash:filename** privileged EXEC command. Depending on the setting of the **file prompt** global configuration command, you might be prompted for confirmation before you delete a file. By default, the access point/bridge prompts for confirmation on destructive file operations. For more information about the **file prompt** command, refer to the *Cisco IOS Command Reference for Release 12.3*.

Working with Software Images

This section describes how to archive (download and upload) software image files, which contain the system software, IOS code, radio firmware, and the web management HTML files.

You download an access point/bridge image file from a TFTP, FTP, or RCP server to upgrade the access point/bridge software. You upload an image file to a TFTP, FTP, or RCP server for backup purposes. You can use this uploaded image for future downloads to the same access point/bridge or another of the same type.

The protocol you use depends on which type of server you are using. The FTP and RCP transport mechanisms provide faster performance and more reliable delivery of data than TFTP. These improvements are possible because FTP and RCP are built on and use the Transmission Control Protocol/Internet Protocol (TCP/IP) stack, which is connection-oriented.

This section includes this information:

- [Image Location on the Access Point/Bridge, page 18-19](#)
- [tar File Format of Images on a Server or Cisco.com, page 18-20](#)
- [Copying Image Files by Using TFTP, page 18-20](#)
- [Copying Image Files by Using FTP, page 18-23](#)
- [Copying Image Files by Using RCP, page 18-28](#)
- [Reloading the Image Using the Web Browser Interface, page 18-33](#)
- [, page 18-34](#)



Note

For a list of software images and supported upgrade paths, refer to the release notes for your access point/bridge.

Image Location on the Access Point/Bridge

The IOS image is stored in a directory that shows the version number. A subdirectory contains the HTML files needed for web management. The image is stored on the system board Flash memory (flash:).

You can use the **show version** privileged EXEC command to see the software version that is currently running on your access point/bridge. In the display, check the line that begins with `System image file is...` It shows the directory name in Flash memory where the image is stored.

You can also use the **dir filesystem:** privileged EXEC command to see the directory names of other software images you might have stored in Flash memory.

tar File Format of Images on a Server or Cisco.com

Software images located on a server or downloaded from Cisco.com are provided in a tar file format, which contains these files:

- *info* file

The *info* file is always at the beginning of the tar file and contains information about the files within it.

- IOS image
- Web management files needed by the HTTP server on the access point/bridge
- radio firmware 6500.img file
- *info.ver* file

The *info.ver* file is always at the end of the tar file and contains the same information as the *info* file. Because it is the last file in the tar file, its existence means that all files in the image have been downloaded.

**Note**

The tar file sometimes ends with an extension other than *.tar*.

Copying Image Files by Using TFTP

You can download an access point/bridge image from a TFTP server or upload the image from the access point/bridge to a TFTP server.

You download an access point/bridge image file from a server to upgrade the access point/bridge software. You can overwrite the current image with the new one.

You upload an access point/bridge image file to a server for backup purposes; this uploaded image can be used for future downloads to the same or another access point/bridge of the same type.

This section includes this information:

- [Preparing to Download or Upload an Image File by Using TFTP, page 18-20](#)
- [Downloading an Image File by Using TFTP, page 18-21](#)
- [Uploading an Image File by Using TFTP, page 18-23](#)

Preparing to Download or Upload an Image File by Using TFTP

Before you begin downloading or uploading an image file by using TFTP, perform these tasks:

- Ensure that the workstation acting as the TFTP server is properly configured. On a Sun workstation, make sure that the */etc/inetd.conf* file contains this line:

```
tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd -p -s /tftpboot
```

Make sure that the */etc/services* file contains this line:

```
tftp 69/udp
```

**Note**

You must restart the inetd daemon after modifying the `/etc/inetd.conf` and `/etc/services` files. To restart the daemon, either stop the inetd process and restart it, or enter a **fastboot** command (on the SunOS 4.x) or a **reboot** command (on Solaris 2.x or SunOS 5.x). For more information on the TFTP daemon, refer to the documentation for your workstation.

- Ensure that the access point/bridge has a route to the TFTP server. The access point/bridge and the TFTP server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the TFTP server by using the **ping** command.
- Ensure that the image to be downloaded is in the correct directory on the TFTP server (usually `/tftpboot` on a UNIX workstation).
- For download operations, ensure that the permissions on the file are set correctly. The permission on the file should be world-read.
- Before uploading the image file, you might need to create an empty file on the TFTP server. To create an empty file, enter the **touch filename** command, where *filename* is the name of the file you will use when uploading the image to the server.
- During upload operations, if you are overwriting an existing file (including an empty file, if you had to create one) on the server, ensure that the permissions on the file are set correctly. Permissions on the file should be world-write.

Downloading an Image File by Using TFTP

You can download a new image file and replace the current image or keep the current image.

**Caution**

For the download and upload algorithms to operate properly, do *not* rename image directories.

Beginning in privileged EXEC mode, follow Steps 1 through 3 to download a new image from a TFTP server and overwrite the existing image.

	Command	Purpose
Step 1	.	Copy the image to the appropriate TFTP directory on the workstation. Make sure the TFTP server is properly configured; see the “Preparing to Download or Upload an Image File by Using TFTP” section on page 18-20
Step 2		Log into the access point/bridge through a Telnet session.

	Command	Purpose
Step 3	archive download-sw /overwrite /reload tftp:[[/location]/directory]/image-name	Download the image file from the TFTP server to the access point/bridge, and overwrite the current image. • The /overwrite option overwrites the software image in Flash with the downloaded image. • The /reload option reloads the system after downloading the image unless the configuration has been changed and not saved. • For <i>//location</i>, specify the IP address of the TFTP server. • For <i>/directory/image-name</i>, specify the directory (optional) and the image to download. Directory and image names are case sensitive.
Step 4	archive download-sw /leave-old-sw /reload tftp:[[/location]/directory]/image-name	Download the image file from the TFTP server to the access point/bridge, and keep the current image. • The /leave-old-sw option keeps the old software version after a download. • The /reload option reloads the system after downloading the image unless the configuration has been changed and not saved. • For <i>//location</i>, specify the IP address of the TFTP server. • For <i>/directory/image-name</i>, specify the directory (optional) and the image to download. Directory and image names are case sensitive.

**Note**

To avoid an unsuccessful download, use the **archive download-sw /safe** command, which downloads the image first and does not delete the current running version until the download succeeds.

The download algorithm verifies that the image is appropriate for the access point/bridge model and that enough DRAM is present, or it aborts the process and reports an error. If you specify the **/overwrite** option, the download algorithm removes the existing image on the Flash device whether or not it is the same as the new one, downloads the new image, and then reloads the software.

**Note**

If the Flash device has sufficient space to hold two images and you want to overwrite one of these images with the same version, you must specify the **/overwrite** option.

If you specify the **/leave-old-sw**, the existing files are not removed. If there is not enough space to install the new image and keep the current running image, the download process stops, and an error message is displayed.

The algorithm installs the downloaded image on the system board Flash device (flash:). The image is placed into a new directory named with the software version string, and the system boot path variable is updated to point to the newly installed image.

If you kept the old image during the download process (you specified the **/leave-old-sw** keyword), you can remove it by entering the **delete /force /recursive filesystem:/file-url** privileged EXEC command. For *filesystem*, use **flash:** for the system board Flash device. For *file-url*, enter the directory name of the old image. All the files in the directory and the directory are removed.

Uploading an Image File by Using TFTP

You can upload an image from the access point/bridge to a TFTP server. You can later download this image to the access point/bridge or to another access point/bridge of the same type.



Caution

For the download and upload algorithms to operate properly, do *not* rename image directories.

Beginning in privileged EXEC mode, follow these steps to upload an image to a TFTP server:

	Command	Purpose
Step 1		Make sure the TFTP server is properly configured; see the “Preparing to Download or Upload an Image File by Using TFTP” section on page 18-20.
Step 1		Log into the access point/bridge through a Telnet session.
Step 2	archive upload-sw tftp:[[/location]/directory]/image-name.tar	Upload the currently running access point/bridge image to the TFTP server. - For <i>[/location]</i>, specify the IP address of the TFTP server. - For <i>/directory/image-name.tar</i>, specify the directory (optional) and the name of the software image to be uploaded. Directory and image names are case sensitive. The <i>image-name.tar</i> is the name of the software image to be stored on the server.

The **archive upload-sw** privileged EXEC command builds an image file on the server by uploading these files in order: info, the IOS image, the HTML files, and info.ver. After these files are uploaded, the upload algorithm creates the tar file format.

Copying Image Files by Using FTP

You can download an access point/bridge image from an FTP server or upload the image from the access point/bridge to an FTP server.

You download an access point/bridge image file from a server to upgrade the access point/bridge software. You can overwrite the current image with the new one or keep the current image after a download.

You upload an access point/bridge image file to a server for backup purposes. You can use this uploaded image for future downloads to the access point/bridge or another access point/bridge of the same type.

This section includes this information:

- [Preparing to Download or Upload an Image File by Using FTP, page 18-24](#)
- [Downloading an Image File by Using FTP, page 18-25](#)
- [Uploading an Image File by Using FTP, page 18-27](#)

Preparing to Download or Upload an Image File by Using FTP

You can copy image files to or from an FTP server.

The FTP protocol requires a client to send a remote username and password on each FTP request to a server. When you copy an image file from the access point/bridge to a server by using FTP, the Cisco IOS software sends the first valid username in this list:

- The username specified in the **archive download-sw** or **archive upload-sw** privileged EXEC command if a username is specified.
- The username set by the **ip ftp username** *username* global configuration command if the command is configured.
- Anonymous.

The access point/bridge sends the first valid password in this list:

- The password specified in the **archive download-sw** or **archive upload-sw** privileged EXEC command if a password is specified.
- The password set by the **ip ftp password** *password* global configuration command if the command is configured.
- The access point/bridge forms a password named *username@apname.domain*. The variable *username* is the username associated with the current session, *apname* is the configured host name, and *domain* is the domain of the access point/bridge.

The username and password must be associated with an account on the FTP server. If you are writing to the server, the FTP server must be properly configured to accept the FTP write request from you.

Use the **ip ftp username** and **ip ftp password** commands to specify a username and password for all copies. Include the username in the **archive download-sw** or **archive upload-sw** privileged EXEC command if you want to specify a username only for that operation.

If the server has a directory structure, the image file is written to or copied from the directory associated with the username on the server. For example, if the image file resides in the home directory of a user on the server, specify that user's name as the remote username.

Before you begin downloading or uploading an image file by using FTP, perform these tasks:

- Ensure that the access point/bridge has a route to the FTP server. The access point/bridge and the FTP server must be in the same subnetwork if you do not have a router to route traffic between subnets. Verify connectivity to the FTP server by using the **ping** command.
- If you are accessing the access point/bridge through a Telnet session and you do not have a valid username, make sure that the current FTP username is the one that you want to use for the FTP download. You can enter the **show users** privileged EXEC command to view the valid username. If you do not want to use this username, create a new FTP username by using the **ip ftp username** *username* global configuration command. This new name will be used during all archive operations. The new username is stored in NVRAM. If you are accessing the access point/bridge through a Telnet session and you have a valid username, this username is used, and you do not need to set the FTP username. Include the username in the **archive download-sw** or **archive upload-sw** privileged EXEC command if you want to specify a username for that operation only.
- When you upload an image file to the FTP server, it must be properly configured to accept the write request from the user on the access point/bridge.

For more information, refer to the documentation for your FTP server.

Downloading an Image File by Using FTP

You can download a new image file and overwrite the current image or keep the current image.

**Caution**

For the download and upload algorithms to operate properly, do *not* rename image directories.

Beginning in privileged EXEC mode, follow Steps 1 through 7 to download a new image from an FTP server and overwrite the existing image. To keep the current image, skip Step 7.

	Command	Purpose
Step 1		Verify that the FTP server is properly configured by referring to the “Preparing to Download or Upload an Image File by Using FTP” section on page 18-24.
Step 2		Log into the access point/bridge through a Telnet session.
Step 3	configure terminal	Enter global configuration mode. This step is required only if you override the default remote username or password (see Steps 4, 5, and 6).
Step 4	ip ftp username <i>username</i>	(Optional) Change the default remote username.
Step 5	ip ftp password <i>password</i>	(Optional) Change the default password.
Step 6	end	Return to privileged EXEC mode.

	Command	Purpose
Step 7	archive download-sw /overwrite /reload ftp:[[/username[:password]@location]/directory] /image-name.tar	Download the image file from the FTP server to the access point/bridge, and overwrite the current image. • The /overwrite option overwrites the software image in Flash with the downloaded image. • The /reload option reloads the system after downloading the image unless the configuration has been changed and not saved. • For //username[:password], specify the username and password; these must be associated with an account on the FTP server. For more information, see the “Preparing to Download or Upload an Image File by Using FTP” section on page 18-24. • For @location, specify the IP address of the FTP server. • For directory/image-name.tar, specify the directory (optional) and the image to download. Directory and image names are case sensitive.
Step 8	archive download-sw /leave-old-sw /reload ftp:[[/username[:password]@location]/directory] /image-name.tar	Download the image file from the FTP server to the access point/bridge, and keep the current image. • The /leave-old-sw option keeps the old software version after a download. • The /reload option reloads the system after downloading the image unless the configuration has been changed and not saved. • For //username[:password], specify the username and password. These must be associated with an account on the FTP server. For more information, see the “Preparing to Download or Upload an Image File by Using FTP” section on page 18-24. • For @location, specify the IP address of the FTP server. • For directory/image-name.tar, specify the directory (optional) and the image to download. Directory and image names are case sensitive.

**Note**

To avoid an unsuccessful download, use the **archive download-sw /safe** command, which downloads the image first and does not delete the current running version until the download succeeds.

The download algorithm verifies that the image is appropriate for the access point/bridge model and that enough DRAM is present, or it aborts the process and reports an error. If you specify the **/overwrite** option, the download algorithm removes the existing image on the Flash device, whether or not it is the same as the new one, downloads the new image, and then reloads the software.

**Note**

If the Flash device has sufficient space to hold two images and you want to overwrite one of these images with the same version, you must specify the **/overwrite** option.

If you specify the **/leave-old-sw**, the existing files are not removed. If there is not enough space to install the new image and keep the running image, the download process stops, and an error message is displayed.

The algorithm installs the downloaded image onto the system board Flash device (flash:). The image is placed into a new directory named with the software version string, and the BOOT path-list is updated to point to the newly installed image. Use the privileged EXEC mode **show boot** command to display boot attributes, and use the global configuration **boot** command to change the boot attributes.

If you kept the old image during the download process (you specified the **/leave-old-sw** keyword), you can remove it by entering the **delete /force /recursive filesystem:/file-url** privileged EXEC command. For *filesystem*, use **flash:** for the system board Flash device. For *file-url*, enter the directory name of the old software image. All the files in the directory and the directory are removed.

Uploading an Image File by Using FTP

You can upload an image from the access point/bridge to an FTP server. You can later download this image to the same access point/bridge or to another access point/bridge of the same type.



Caution

For the download and upload algorithms to operate properly, do *not* rename image directories.

The upload feature is available only if the HTML pages associated with the Cluster Management Suite (CMS) have been installed with the existing image.

Beginning in privileged EXEC mode, follow these steps to upload an image to an FTP server:

	Command	Purpose
Step 1		Verify that the FTP server is properly configured by referring to the “Preparing to Download or Upload a Configuration File by Using FTP” section on page 18-13.
Step 2		Log into the access point/bridge through a Telnet session.
Step 3	configure terminal	Enter global configuration mode. This step is required only if you override the default remote username or password (see Steps 4, 5, and 6).
Step 4	ip ftp username <i>username</i>	(Optional) Change the default remote username.
Step 5	ip ftp password <i>password</i>	(Optional) Change the default password.

	Command	Purpose
Step 6	end	Return to privileged EXEC mode.
Step 7	archive upload-sw ftp:[[/[username[:password]@]location]/directory]/ image-name.tar	Upload the currently running access point/bridge image to the FTP server. - For <i>//username:password</i>, specify the username and password. These must be associated with an account on the FTP server. For more information, see the “Preparing to Download or Upload an Image File by Using FTP” section on page 18-24. - For <i>@location</i>, specify the IP address of the FTP server. - For <i>/directory/image-name.tar</i>, specify the directory (optional) and the name of the software image to be uploaded. Directory and image names are case sensitive. The <i>image-name.tar</i> is the name of the software image to be stored on the server.

The **archive upload-sw** command builds an image file on the server by uploading these files in order: info, the IOS image, the HTML files, and info.ver. After these files are uploaded, the upload algorithm creates the tar file format.

Copying Image Files by Using RCP

You can download an access point/bridge image from an RCP server or upload the image from the access point/bridge to an RCP server.

You download an access point/bridge image file from a server to upgrade the access point/bridge software. You can overwrite the current image with the new one or keep the current image after a download.

You upload an access point/bridge image file to a server for backup purposes. You can use this uploaded image for future downloads to the same access point/bridge or another of the same type.

This section includes this information:

- [Preparing to Download or Upload an Image File by Using RCP, page 18-28](#)
- [Downloading an Image File by Using RCP, page 18-30](#)
- [Uploading an Image File by Using RCP, page 18-32](#)

Preparing to Download or Upload an Image File by Using RCP

RCP provides another method of downloading and uploading image files between remote hosts and the access point/bridge. Unlike TFTP, which uses User Datagram Protocol (UDP), a connectionless protocol, RCP uses TCP, which is connection-oriented.

To use RCP to copy files, the server from or to which you will be copying files must support RCP. The RCP copy commands rely on the rsh server (or daemon) on the remote system. To copy files by using RCP, you do not need to create a server for file distribution as you do with TFTP. You only need to have access to a server that supports the remote shell (rsh). (Most UNIX systems support rsh.) Because you are copying a file from one place to another, you must have read permission on the source file and write permission on the destination file. If the destination file does not exist, RCP creates it for you.

RCP requires a client to send a remote username on each RCP request to a server. When you copy an image from the access point/bridge to a server by using RCP, the Cisco IOS software sends the first valid username in this list:

- The username specified in the **archive download-sw** or **archive upload-sw** privileged EXEC command if a username is specified.
- The username set by the **ip rcmd remote-username** *username* global configuration command if the command is entered.
- The remote username associated with the current TTY (terminal) process. For example, if the user is connected to the router through Telnet and was authenticated through the **username** command, the access point/bridge software sends the Telnet username as the remote username.
- The access point/bridge host name.

For the RCP copy request to execute successfully, an account must be defined on the network server for the remote username. If the server has a directory structure, the image file is written to or copied from the directory associated with the remote username on the server. For example, if the image file resides in the home directory of a user on the server, specify that user's name as the remote username.

Before you begin downloading or uploading an image file by using RCP, do these tasks:

- Ensure that the workstation acting as the RCP server supports the remote shell (rsh).
- Ensure that the access point/bridge has a route to the RCP server. The access point/bridge and the server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the RCP server by using the **ping** command.
- If you are accessing the access point/bridge through a Telnet session and you do not have a valid username, make sure that the current RCP username is the one that you want to use for the RCP download. You can enter the **show users** privileged EXEC command to view the valid username. If you do not want to use this username, create a new RCP username by using the **ip rcmd remote-username** *username* global configuration command to be used during all archive operations. The new username is stored in NVRAM. If you are accessing the access point/bridge through a Telnet session and you have a valid username, this username is used, and there is no need to set the RCP username. Include the username in the **archive download-sw** or **archive upload-sw** privileged EXEC command if you want to specify a username only for that operation.
- When you upload an image to the RCP to the server, it must be properly configured to accept the RCP write request from the user on the access point/bridge. For UNIX systems, you must add an entry to the `.rhosts` file for the remote user on the RCP server. For example, suppose the access point/bridge contains these configuration lines:

```
hostname ap1
ip rcmd remote-username User0
```

If the access point/bridge IP address translates to *ap1.company.com*, the `.rhosts` file for User0 on the RCP server should contain this line:

```
ap1.company.com ap1
```

For more information, refer to the documentation for your RCP server.

Downloading an Image File by Using RCP

You can download a new image file and replace or keep the current image.



Caution

For the download and upload algorithms to operate properly, do *not* rename image directories.

Beginning in privileged EXEC mode, follow Steps 1 through 6 to download a new image from an RCP server and overwrite the existing image. To keep the current image, skip Step 6.

	Command	Purpose
Step 1		Verify that the RCP server is properly configured by referring to the “Preparing to Download or Upload an Image File by Using RCP” section on page 18-28.
Step 2		Log into the access point/bridge through a Telnet session.
Step 3	configure terminal	Enter global configuration mode. This step is required only if you override the default remote username (see Steps 4 and 5).
Step 4	ip rcmd remote-username <i>username</i>	(Optional) Specify the remote username.
Step 5	end	Return to privileged EXEC mode.
Step 6	archive download-sw /overwrite /reload rcp: [[[//[username@]location]/directory]/image-name.tar]	Download the image file from the RCP server to the access point/bridge, and overwrite the current image. • The /overwrite option overwrites the software image in Flash with the downloaded image. • The /reload option reloads the system after downloading the image unless the configuration has been changed and not saved. • For <i>//username</i>, specify the username. For the RCP copy request to execute successfully, an account must be defined on the network server for the remote username. For more information, see the “Preparing to Download or Upload an Image File by Using RCP” section on page 18-28. • For <i>@location</i>, specify the IP address of the RCP server. • For <i>/directory/image-name.tar</i>, specify the directory (optional) and the image to download. Directory and image names are case sensitive.

	Command	Purpose
Step 7	archive download-sw /leave-old-sw /reload rcp:[[/[[username@]location]/directory]/image-name.tar]	Download the image file from the RCP server to the access point/bridge, and keep the current image. • The /leave-old-sw option keeps the old software version after a download. • The /reload option reloads the system after downloading the image unless the configuration has been changed and not saved. • For <i>//username</i>, specify the username. For the RCP copy request to execute, an account must be defined on the network server for the remote username. For more information, see the “Preparing to Download or Upload an Image File by Using RCP” section on page 18-28. • For <i>@location</i>, specify the IP address of the RCP server. • For <i>/directory]/image-name.tar</i>, specify the directory (optional) and the image to download. Directory and image names are case sensitive.

**Note**

To avoid an unsuccessful download, use the **archive download-sw /safe** command, which downloads the image first and does not delete the current running version until the download succeeds.

The download algorithm verifies that the image is appropriate for the access point/bridge model and that enough DRAM is present, or it aborts the process and reports an error. If you specify the **/overwrite** option, the download algorithm removes the existing image on the Flash device whether or not it is the same as the new one, downloads the new image, and then reloads the software.

**Note**

If the Flash device has sufficient space to hold two images and you want to overwrite one of these images with the same version, you must specify the **/overwrite** option.

If you specify the **/leave-old-sw**, the existing files are not removed. If there is not enough room to install the new image and keep the running image, the download process stops, and an error message is displayed.

The algorithm installs the downloaded image onto the system board Flash device (flash:). The image is placed into a new directory named with the software version string, and the BOOT environment variable is updated to point to the newly installed image.

If you kept the old software during the download process (you specified the **/leave-old-sw** keyword), you can remove it by entering the **delete /force /recursive filesystem:/file-url** privileged EXEC command. For *filesystem*, use **flash:** for the system board Flash device. For *file-url*, enter the directory name of the old software image. All the files in the directory and the directory are removed.

Uploading an Image File by Using RCP

You can upload an image from the access point/bridge to an RCP server. You can later download this image to the same access point/bridge or to another access point/bridge of the same type.



Caution

For the download and upload algorithms to operate properly, do *not* rename image directories.

The upload feature is available only if the HTML pages associated with the Cluster Management Suite (CMS) have been installed with the existing image.

Beginning in privileged EXEC mode, follow these steps to upload an image to an RCP server:

	Command	Purpose
Step 1		Verify that the RCP server is properly configured by referring to the “Preparing to Download or Upload an Image File by Using RCP” section on page 18-28.
Step 2		Log into the access point/bridge through a Telnet session.
Step 3	configure terminal	Enter global configuration mode. This step is required only if you override the default remote username (see Steps 4 and 5).
Step 4	ip rcmd remote-username <i>username</i>	(Optional) Specify the remote username.
Step 5	end	Return to privileged EXEC mode.
Step 6	archive upload-sw rcp: [[[// <i>[username@]</i> <i>location</i>]/ <i>directory</i>]/ <i>image-name.tar</i>]	Upload the currently running access point/bridge image to the RCP server. - For <i>//username</i>, specify the username; for the RCP copy request to execute, an account must be defined on the network server for the remote username. For more information, see the “Preparing to Download or Upload an Image File by Using RCP” section on page 18-28. - For <i>@location</i>, specify the IP address of the RCP server. - For <i>/directory</i>]/<i>image-name.tar</i>, specify the directory (optional) and the name of the software image to be uploaded. Directory and image names are case sensitive. - The <i>image-name.tar</i> is the name of software image to be stored on the server.

The **archive upload-sw** privileged EXEC command builds an image file on the server by uploading these files in order: info, the IOS image, the HTML files, and info.ver. After these files are uploaded, the upload algorithm creates the tar file format.

Reloading the Image Using the Web Browser Interface

You can also use the Web browser interface to reload the access point/bridge image file. The Web browser interface supports loading the image file using HTTP or TFTP interfaces.



Note Your access point/bridge configuration is not changed when using the browser to reload the image file.

Browser HTTP Interface

The HTTP interface allows you to browse to the access point/bridge image file on your PC and download the image to the access point/bridge. Follow the instructions below to use the HTTP interface:

- Step 1** Open your Internet browser. You must use Microsoft Internet Explorer (version 5.x or later) or Netscape Navigator (version 4.x).
- Step 2** Enter the access point/bridge's IP address in the browser address line and press **Enter**. An Enter Network Password screen appears.
- Step 3** Enter your username in the User Name field.
- Step 4** Enter the access point/bridge password in the Password field and press **Enter**. The Summary Status page appears.
- Step 5** Click the **System Software** tab and then click **Software Upgrade**. The HTTP Upgrade screen appears.
- Step 6** Click the **Browse** button to locate the image file on your PC.
- Step 7** Click the **Upload** button.

For additional information, click the **Help** icon on the Software Upgrade screen.

Browser TFTP Interface

The TFTP interface allows you to use a TFTP server on a network device to load the access point/bridge image file. Follow the instructions below to use a TFTP server:

- Step 1** Open your Internet browser. You must use Microsoft Internet Explorer (version 5.x or later) or Netscape Navigator (version 4.x).
- Step 2** Enter the access point/bridge's IP address in the browser address line and press **Enter**. An Enter Network Password screen appears.
- Step 3** Enter your username in the User Name field.
- Step 4** Enter the access point/bridge password in the Password field and press **Enter**. The Summary Status page appears.
- Step 5** Click the **System Software** tab and then click **Software Upgrade**. The HTTP Upgrade screen appears.
- Step 6** Click the **TFTP Upgrade** tab.
- Step 7** Enter the IP address for the TFTP server in the TFTP Server field.

Step 8 Enter the file name for the access point/bridge image file in the Upload New System Image Tar File field. If the file is located in a subdirectory of the TFTP server root directory, include the relative path of the TFTP server root directory with the filename. If the file is located in the TFTP root directory, enter only the filename.

Step 9 Click the **Upload** button.

For additional information click the Help icon on the Software Upgrade screen.



CHAPTER 19

Configuring System Message Logging

This chapter describes how to configure system message logging on your access point/bridge.



Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Cisco IOS Configuration Fundamentals Command Reference for Release 12.3*.

This chapter consists of these sections:

- [Understanding System Message Logging, page 19-2](#)
- [Configuring System Message Logging, page 19-2](#)
- [Displaying the Logging Configuration, page 19-12](#)

Understanding System Message Logging

By default, access point/bridges send the output from system messages and **debug** privileged EXEC commands to a logging process. The logging process controls the distribution of logging messages to various destinations, such as the logging buffer, terminal lines, or a UNIX syslog server, depending on your configuration. The process also sends messages to the console.

**Note**

The syslog format is compatible with 4.3 BSD UNIX.

When the logging process is disabled, messages are sent only to the console. The messages are sent as they are generated, so message and debug output are interspersed with prompts or output from other commands. Messages are displayed on the console after the process that generated them has finished.

You can set the severity level of the messages to control the type of messages displayed on the console and each of the destinations. You can timestamp log messages or set the syslog source address to enhance real-time debugging and management.

You can access logged system messages by using the access point/bridge command-line interface (CLI) or by saving them to a properly configured syslog server. The access point/bridge software saves syslog messages in an internal buffer. You can remotely monitor system messages by accessing the access point/bridge through Telnet or by viewing the logs on a syslog server.

Configuring System Message Logging

This section describes how to configure system message logging. It contains this configuration information:

- [System Log Message Format, page 19-2](#)
- [Default System Message Logging Configuration, page 19-3](#)
- [Disabling and Enabling Message Logging, page 19-4](#)
- [Setting the Message Display Destination Device, page 19-5](#)
- [Enabling and Disabling Timestamps on Log Messages, page 19-6](#)
- [Enabling and Disabling Sequence Numbers in Log Messages, page 19-6](#)
- [Defining the Message Severity Level, page 19-7](#)
- [Limiting Syslog Messages Sent to the History Table and to SNMP, page 19-8](#)
- [Setting a Logging Rate Limit, page 19-9](#)
- [Configuring UNIX Syslog Servers, page 19-10](#)

System Log Message Format

System log messages can contain up to 80 characters and a percent sign (%), which follows the optional sequence number or timestamp information, if configured. Messages are displayed in this format:

seq no:timestamp: %facility-severity-MNEMONIC:description

The part of the message preceding the percent sign depends on the setting of the **service sequence-numbers**, **service timestamps log datetime**, **service timestamps log datetime [localtime] [msec] [show-timezone]**, or **service timestamps log uptime** global configuration command.

Table 19-1 describes the elements of syslog messages.

Table 19-1 System Log Message Elements

Element	Description
<i>seq no:</i>	Stamps log messages with a sequence number only if the service sequence-numbers global configuration command is configured. For more information, see the “ Enabling and Disabling Sequence Numbers in Log Messages ” section on page 19-6.
<i>timestamp</i> formats: <i>mm/dd hh:mm:ss</i> or <i>hh:mm:ss</i> (short uptime) or <i>d h</i> (long uptime)	Date and time of the message or event. This information appears only if the service timestamps log [datetime log] global configuration command is configured. For more information, see the “ Enabling and Disabling Timestamps on Log Messages ” section on page 19-6.
<i>facility</i>	The facility to which the message refers (for example, SNMP, SYS, and so forth). A facility can be a hardware device, a protocol, or a module of the system software. It denotes the source or the cause of the system message.
<i>severity</i>	Single-digit code from 0 to 7 that is the severity of the message. For a description of the severity levels, see Table 19-3 on page 19-8 .
<i>MNEMONIC</i>	Text string that uniquely describes the message.
<i>description</i>	Text string containing detailed information about the event being reported.

This example shows a partial access point/bridge system message:

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet0/2, changed state to up
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed
state to down 2
*Mar  1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
18:47:02: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
*Mar  1 18:48:50.483 UTC: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
```

Default System Message Logging Configuration

Table 19-2 shows the default system message logging configuration.

Table 19-2 Default System Message Logging Configuration

Feature	Default Setting
System message logging to the console	Enabled
Console severity	Debugging (and numerically lower levels; see Table 19-3 on page 19-8)
Logging buffer size	4096 bytes
Logging history size	1 message

Table 19-2 **Default System Message Logging Configuration (continued)**

Feature	Default Setting
Timestamps	Disabled
Synchronous logging	Disabled
Logging server	Disabled
Syslog server IP address	None configured
Server facility	Local7 (see Table 19-4 on page 19-11)
Server severity	Informational (and numerically lower levels; see Table 19-3 on page 19-8)

Disabling and Enabling Message Logging

Message logging is enabled by default. It must be enabled to send messages to any destination other than the console. When enabled, log messages are sent to a logging process, which logs messages to designated locations asynchronously to the processes that generated the messages.

Beginning in privileged EXEC mode, follow these steps to disable message logging:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	no logging on	Disable message logging.
Step 3	end	Return to privileged EXEC mode.
Step 4	show running-config or show logging	Verify your entries.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Disabling the logging process can slow down the access point/bridge because a process must wait until the messages are written to the console before continuing. When the logging process is disabled, messages are displayed on the console as soon as they are produced, often appearing in the middle of command output.

The **logging synchronous** global configuration command also affects the display of messages to the console. When this command is enabled, messages appear only after you press Return. For more information, see the “[Enabling and Disabling Timestamps on Log Messages](#)” section on page 19-6.

To re-enable message logging after it has been disabled, use the **logging on** global configuration command.

Setting the Message Display Destination Device

If message logging is enabled, you can send messages to specific locations in addition to the console. Beginning in privileged EXEC mode, use one or more of the following commands to specify the locations that receive messages:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	logging buffered <i>[size]</i> <i>[level]</i>	Log messages to an internal buffer. The default buffer size is 4096. The range is 4096 to 2147483647 bytes. Levels include emergencies 0, alerts 1, critical 2, errors 3, warnings 4, notifications 5, informational 6, and debugging 7. Note Do not make the buffer size too large because the access point/bridge could run out of memory for other tasks. Use the show memory privileged EXEC command to view the free processor memory on the access point/bridge; however, this value is the maximum available, and you should <i>not</i> set the buffer size to this amount.
Step 3	logging <i>host</i>	Log messages to a UNIX syslog server host. For <i>host</i> , specify the name or IP address of the host to be used as the syslog server. To build a list of syslog servers that receive logging messages, enter this command more than once. For complete syslog server configuration steps, see the “Configuring UNIX Syslog Servers” section on page 19-10 .
Step 4	end	Return to privileged EXEC mode.
Step 5	terminal monitor	Log messages to a non-console terminal during the current session. Terminal parameter-setting commands are set locally and do not remain in effect after the session has ended. You must perform this step for each session to see the debugging messages.
Step 6	show running-config	Verify your entries.
Step 7	copy running-config startup-config	(Optional) Save your entries in the configuration file.

The **logging buffered** global configuration command copies logging messages to an internal buffer. The buffer is circular, so newer messages overwrite older messages after the buffer is full. To display the messages that are logged in the buffer, use the **show logging** privileged EXEC command. The first message displayed is the oldest message in the buffer. To clear the contents of the buffer, use the **clear logging** privileged EXEC command.

To disable logging to the console, use the **no logging console** global configuration command. To disable logging to a file, use the **no logging file** *[severity-level-number | type]* global configuration command.

Enabling and Disabling Timestamps on Log Messages

By default, log messages are not timestamped.

Beginning in privileged EXEC mode, follow these steps to enable timestamping of log messages:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	service timestamps log uptime or service timestamps log datetime [msec] [localtime] [show-timezone]	Enable log timestamps. The first command enables timestamps on log messages, showing the time since the system was rebooted. The second command enables timestamps on log messages. Depending on the options selected, the timestamp can include the date, time in milliseconds relative to the local time zone, and the time zone name.
Step 3	end	Return to privileged EXEC mode.
Step 4	show running-config	Verify your entries.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To disable timestamps for both debug and log messages, use the **no service timestamps** global configuration command.

This example shows part of a logging display with the **service timestamps log datetime** global configuration command enabled:

```
*Mar  1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
```

This example shows part of a logging display with the **service timestamps log uptime** global configuration command enabled:

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
```

Enabling and Disabling Sequence Numbers in Log Messages

Because there is a chance that more than one log message can have the same timestamp, you can display messages with sequence numbers so that you can unambiguously refer to a single message. By default, sequence numbers in log messages are not displayed.

Beginning in privileged EXEC mode, follow these steps to enable sequence numbers in log messages:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	service sequence-numbers	Enable sequence numbers.
Step 3	end	Return to privileged EXEC mode.
Step 4	show running-config	Verify your entries.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To disable sequence numbers, use the **no service sequence-numbers** global configuration command.

This example shows part of a logging display with sequence numbers enabled:

```
000019: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
```

Defining the Message Severity Level

You can limit messages displayed to the selected device by specifying the severity level of the message, which are described in [Table 19-3](#).

Beginning in privileged EXEC mode, follow these steps to define the message severity level:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	logging console <i>level</i>	Limit messages logged to the console. By default, the console receives debugging messages and numerically lower levels (see Table 19-3 on page 19-8).
Step 3	logging monitor <i>level</i>	Limit messages logged to the terminal lines. By default, the terminal receives debugging messages and numerically lower levels (see Table 19-3 on page 19-8).
Step 4	logging trap <i>level</i>	Limit messages logged to the syslog servers. By default, syslog servers receive informational messages and numerically lower levels (see Table 19-3 on page 19-8). For complete syslog server configuration steps, see the “ Configuring UNIX Syslog Servers ” section on page 19-10.
Step 5	end	Return to privileged EXEC mode.
Step 6	show running-config or show logging	Verify your entries.
Step 7	copy running-config startup-config	(Optional) Save your entries in the configuration file.



Note

Specifying a *level* causes messages at that level and numerically lower levels to be displayed at the destination.

To disable logging to the console, use the **no logging console** global configuration command. To disable logging to a terminal other than the console, use the **no logging monitor** global configuration command. To disable logging to syslog servers, use the **no logging trap** global configuration command.

Table 19-3 describes the *level* keywords. It also lists the corresponding UNIX syslog definitions from the most severe level to the least severe level.

Table 19-3 Message Logging Level Keywords

Level Keyword	Level	Description	Syslog Definition
emergencies	0	System unstable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR
warnings	4	Warning conditions	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

The software generates four other categories of messages:

- Error messages about software or hardware malfunctions, displayed at levels **warnings** through **emergencies**. These types of messages mean that the functionality of the access point/bridge is affected.
- Output from the **debug** commands, displayed at the **debugging** level. Debug commands are typically used only by the Technical Assistance Center (TAC).
- Interface up or down transitions and system restart messages, displayed at the **notifications** level. This message is only for information; access point/bridge functionality is not affected.
- Reload requests and low-process stack messages, displayed at the **informational** level. This message is only for information; access point/bridge functionality is not affected.

Limiting Syslog Messages Sent to the History Table and to SNMP

If you have enabled syslog message traps to be sent to an SNMP network management station by using the **snmp-server enable trap** global configuration command, you can change the level of messages sent and stored in the access point/bridge history table. You can also change the number of messages that are stored in the history table.

Messages are stored in the history table because SNMP traps are not guaranteed to reach their destination. By default, one message of the level **warning** and numerically lower levels (see Table 19-3 on page 19-8) are stored in the history table even if syslog traps are not enabled.

Beginning in privileged EXEC mode, follow these steps to change the level and history table size defaults:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	logging history <i>level</i> ¹	Change the default level of syslog messages stored in the history file and sent to the SNMP server. See Table 19-3 on page 19-8 for a list of <i>level</i> keywords. By default, warnings , errors , critical , alerts , and emergencies messages are sent.
Step 3	logging history size <i>number</i>	Specify the number of syslog messages that can be stored in the history table. The default is to store one message. The range is 1 to 500 messages.
Step 4	end	Return to privileged EXEC mode.
Step 5	show running-config	Verify your entries.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

1. [Table 19-3](#) lists the level keywords and severity level. For SNMP usage, the severity level values increase by 1. For example, emergencies equal 1, not 0, and critical equals 3, not 2.

When the history table is full (it contains the maximum number of message entries specified with the **logging history size** global configuration command), the oldest message entry is deleted from the table to allow the new message entry to be stored.

To return the logging of syslog messages to the default level, use the **no logging history** global configuration command. To return the number of messages in the history table to the default value, use the **no logging history size** global configuration command.

Setting a Logging Rate Limit

You can enable a limit on the number of messages that the access point/bridge logs per second. You can enable the limit for all messages or for messages sent to the console, and you can specify that messages of a specific severity are exempt from the limit.

Beginning in privileged EXEC mode, follow these steps to enable a logging rate limit:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	logging rate-limit <i>seconds</i> [all console] [except <i>severity</i>]	Enable a logging rate limit in seconds. (Optional) Apply the limit to all logging or only to messages logged to the console. (Optional) Exempt a specific severity from the limit.
Step 3	end	Return to privileged EXEC mode.
Step 4	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To disable the rate limit, use the **no logging rate-limit** global configuration command.

Configuring UNIX Syslog Servers

The next sections describe how to configure the 4.3 BSD UNIX server syslog daemon and define the UNIX system logging facility.

Logging Messages to a UNIX Syslog Daemon

Before you can send system log messages to a UNIX syslog server, you must configure the syslog daemon on a UNIX server. Log in as root, and perform these steps:

**Note**

Some recent versions of UNIX syslog daemons no longer accept by default syslog packets from the network. If this is the case with your system, use the UNIX **man syslogd** command to determine what options must be added to or removed from the syslog command line to enable logging of remote syslog messages.

Step 1 Add a line such as the following to the file `/etc/syslog.conf`:

```
local7.debug /usr/adm/log/cisco.log
```

The **local7** keyword specifies the logging facility to be used; see [Table 19-4 on page 19-11](#) for information on the facilities. The **debug** keyword specifies the syslog level; see [Table 19-3 on page 19-8](#) for information on the severity levels. The syslog daemon sends messages at this level or at a more severe level to the file specified in the next field. The file must already exist, and the syslog daemon must have permission to write to it.

Step 2 Create the log file by entering these commands at the UNIX shell prompt:

```
$ touch /usr/adm/log/cisco.log
$ chmod 666 /usr/adm/log/cisco.log
```

Step 3 Make sure the syslog daemon reads the new changes by entering this command:

```
$ kill -HUP `cat /etc/syslog.pid`
```

For more information, see the **man syslog.conf** and **man syslogd** commands on your UNIX system.

Configuring the UNIX System Logging Facility

When sending system log messages to an external device, you can cause the access point/bridge to identify its messages as originating from any of the UNIX syslog facilities.

Beginning in privileged EXEC mode, follow these steps to configure UNIX system facility message logging:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	logging host	Log messages to a UNIX syslog server host by entering its IP address. To build a list of syslog servers that receive logging messages, enter this command more than once.

	Command	Purpose
Step 3	logging trap <i>level</i>	Limit messages logged to the syslog servers. By default, syslog servers receive informational messages and lower. See Table 19-3 on page 19-8 for <i>level</i> keywords.
Step 4	logging facility <i>facility-type</i>	Configure the syslog facility. See Table 19-4 on page 19-11 for <i>facility-type</i> keywords. The default is local7 .
Step 5	end	Return to privileged EXEC mode.
Step 6	show running-config	Verify your entries.
Step 7	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To remove a syslog server, use the **no logging host** global configuration command, and specify the syslog server IP address. To disable logging to syslog servers, enter the **no logging trap** global configuration command.

[Table 19-4](#) lists the 4.3 BSD UNIX system facilities supported by the Cisco IOS software. For more information about these facilities, consult the operator's manual for your UNIX operating system.

Table 19-4 Logging Facility-Type Keywords

Facility Type Keyword	Description
auth	Authorization system
cron	Cron facility
daemon	System daemon
kern	Kernel
local0-7	Locally defined messages
lpr	Line printer system
mail	Mail system
news	USENET news
sys9	System use
sys10	System use
sys11	System use
sys12	System use
sys13	System use
sys14	System use
syslog	System log
user	User process
uucp	UNIX-to-UNIX copy system

Displaying the Logging Configuration

To display the current logging configuration and the contents of the log buffer, use the **show logging** privileged EXEC command. For information about the fields in this display, refer to the *Cisco IOS Configuration Fundamentals Command Reference for Release 12.3*.

To display the logging history file, use the **show logging history** privileged EXEC command.



Configuring Repeater and Standby Access Points and Workgroup Bridge Mode

This chapter describes how to configure your access point as a repeater, as a hot standby unit, or as a workgroup bridge. This chapter contains these sections:

- [Understanding Repeater Access Points, page 20-2](#)
- [Configuring a Repeater Access Point, page 20-3](#)
- [Understanding Workgroup Bridge Mode, page 20-11](#)
- [Configuring Workgroup Bridge Mode, page 20-13](#)

Understanding Repeater Access Points

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

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. When you configure the access point/bridge as a repeater, the access point's Ethernet port does not forward traffic.

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

A repeater access point associates to the access point with which it has the best connectivity. However, you can specify the access point to which the repeater associates. Setting up a static, specific association between a repeater and a root access point improves repeater performance.

To set up repeaters, you must enable Aironet extensions on both the parent (root) access point and the repeater access points. Aironet extensions, which are enabled by default, improve the access point's ability to understand the capabilities of Cisco Aironet client devices associated with the access point. Disabling Aironet extensions sometimes improves the interoperability between the access point and non-Cisco client devices. Non-Cisco client devices might have difficulty communicating with repeater access points and the root access point to which repeaters are associated.



Note

Because the access point/bridge creates a virtual interface for its radio interface, repeater access points associate to the root access point twice: once for the actual interface and once for the virtual interface.

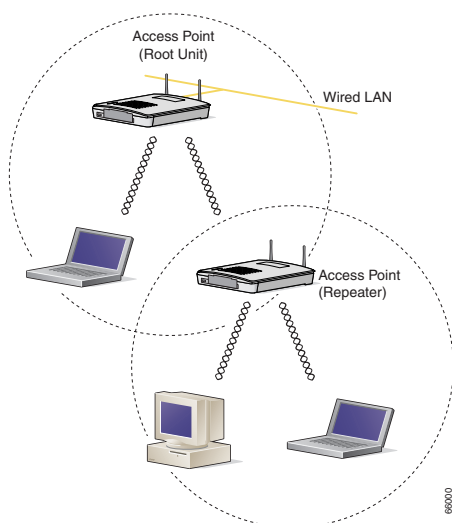


Note

You cannot configure multiple VLANs on repeater access points. Repeater access points support only the native VLAN.

Figure 20-1 shows an access point acting as a repeater.

Figure 20-1 Access Point as a Repeater



Configuring a Repeater Access Point

This section provides instructions for setting up an access point as a repeater and includes these sections:

- [Default Configuration, page 20-3](#)
- [Guidelines for Repeaters, page 20-3](#)
- [Setting Up a Repeater, page 20-4](#)
- [Verifying Repeater Operation, page 20-5](#)
- [Setting Up a Repeater As a LEAP Client, page 20-5](#)
- [Setting Up a Repeater As a WPA Client, page 20-6](#)

Default Configuration

The access point/bridge boots in the Root AP mode by default. [Table 20-1](#) shows the default values for settings that control the access point's role in the wireless LAN.

Table 20-1 *Default Settings for Role in Wireless LAN*

Feature	Default Setting
Station role	Root AP
Optimize Radio Network for	Default
Extensions	Aironet

Guidelines for Repeaters

Follow these guidelines when configuring repeater access points:

- Use repeaters to serve client devices that do not require high throughput. Repeaters extend the coverage area of your wireless LAN, but they drastically reduce throughput.
- Use repeaters when most if not all client devices that associate with the repeaters are Cisco Aironet clients. Non-Cisco client devices sometimes have trouble communicating with repeater access points.
- Make sure that the data rates configured on the repeater access point match the data rates on the parent access point. For instructions on configuring data rates, see the [“Configuring Radio Data Rates” section on page 6-5](#).
- Repeater access points support only the native VLAN. You cannot configure multiple VLANs on a repeater access point.

**Note**

Repeater access points running Cisco IOS software cannot associate to parent access points that do not run Cisco IOS software.

**Note**

Repeater access points do not support wireless domain services (WDS). Do not configure a repeater access point as a WDS candidate, and do not configure a WDS access point to fall back to repeater mode in case of Ethernet failure.

**Note**

If multiple BSSIDs are configured on a root access point that is designated as the parent of a repeater, the parent MAC address might change if a BSSID on the parent is added or deleted. If you use multiple BSSIDs on your wireless LAN and a repeater on your wireless LAN is configured to associate to a specific parent, check the association status of the repeater when you add or delete BSSIDs on the parent access point.

Setting Up a Repeater

Beginning in Privileged Exec mode, follow these steps to configure an access point as a repeater:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.
Step 3	ssid <i>ssid-string</i>	Create the SSID that the repeater uses to associate to a root access point; in the next step designate this SSID as an infrastructure SSID. If you created an infrastructure SSID on the root access point, create the same SSID on the repeater, also.
Step 4	infrastructure-ssid [optional]	Designate the SSID as an infrastructure SSID. The repeater uses this SSID to associate to the root access point. Infrastructure devices must associate to the repeater access point using this SSID unless you also enter the optional keyword.
Step 5	exit	Exit SSID configuration mode and return to radio interface configuration mode.
Step 6	station-role repeater	Set the access point's role in the wireless LAN to repeater.
Step 7	dot11 extensions aironet	If Aironet extensions are disabled, enable Aironet extensions.
Step 8	parent {1-4} <i>mac-address</i> [timeout]	(Optional) Enter the MAC address for the access point to which the repeater should associate. - You can enter MAC addresses for up to four parent access points. The repeater attempts to associate to MAC address 1 first; if that access point does not respond, the repeater tries the next access point in its parent list. Note If multiple BSSIDs are configured on the parent access point, the MAC address for the parent might change if a BSSID on the parent is added or deleted. (Optional) You can also enter a timeout value in seconds that determines how long the repeater attempts to associate to a parent access point before trying the next parent in the list. Enter a timeout value from 0 to 65535 seconds.
Step 9	end	Return to privileged EXEC mode.
Step 10	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to set up a repeater access point with three potential parents:

```

ap# configure terminal
ap(config)# interface dot11radio 0
ap(config-if)# ssid chicago
ap(config-ssid)# infrastructure-ssid
ap(config-ssid)# exit
ap(config-if)# station-role repeater
ap(config-if)# dot11 extensions aironet
ap(config-if)# parent 1 0987.1234.h345 900
ap(config-if)# parent 2 7809.b123.c345 900
ap(config-if)# parent 3 6543.a456.7421 900
ap(config-if)# end

```

Verifying Repeater Operation

After you set up the repeater, check the access point/bridge LEDs. If your repeater is functioning correctly, the LEDs on the repeater and the root access point to which it is associated behave like this:

- The status LED on the root access point is steady green, indicating that at least one client device is associated with it (in this case, the repeater).
- The status LED on the repeater access point is steady green when it is associated with the root access point and the repeater has client devices associated to it. The repeater's status LED flashes (steady green for 7/8 of a second and off for 1/8 of a second) when it is associated with the root access point but the repeater has no client devices associated to it.

The repeater access point should also appear as associated with the root access point in the root access point's Association Table.

Setting Up a Repeater As a LEAP Client

You can set up a 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.

Setting up a repeater as a LEAP client requires three major steps:

1. Create an authentication username and password for the repeater on your authentication server.
2. Configure LEAP authentication on the root access point to which the repeater associates. The access point to which the repeater associates is called the parent access point. See [Chapter 10, "Configuring Authentication Types,"](#) for instructions on setting up authentication.



Note

On the repeater access point, you must enable the same cipher suite or WEP encryption method and WEP features that are enabled on the parent access point.

3. Configure the repeater to act as a LEAP client. Beginning in Privileged Exec mode, follow these instructions to set up the repeater as a LEAP client:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.

	Command	Purpose
Step 3	ssid <i>ssid-string</i>	Create an SSID and enter SSID configuration mode for the new SSID. The SSID can consist of up to 32 alphanumeric characters, but they should not include spaces. SSIDs are case-sensitive.
Step 4	authentication network-eap <i>list-name</i>	Enable LEAP authentication on the repeater so that LEAP-enabled client devices can authenticate through the repeater. For list-name, specify the list name you want to use for EAP authentication. You define list names for EAP and for MAC addresses using the aaa authentication login command. These lists define the authentication methods activated when a user logs in and indirectly identify the location where the authentication information is stored.
Step 5	authentication client username <i>username</i> password <i>password</i>	Configure the username and password that the repeater uses when it performs LEAP authentication. This username and password must match the username and password that you set up for the repeater on the authentication server.
Step 6	infrastructure ssid [optional]	(Optional) Designate the SSID as the SSID that other access points and workgroup bridges use to associate to this access point. If you do not designate an SSID as the infrastructure SSID, infrastructure devices can associate to the access point using any SSID. If you designate an SSID as the infrastructure SSID, infrastructure devices must associate to the access point using that SSID unless you also enter the optional keyword.
Step 7	end	Return to privileged EXEC mode.
Step 8	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Setting Up a Repeater As a WPA Client

WPA key management uses a combination of encryption methods to protect communication between client devices and the access point. You can set up a repeater access point to authenticate to your network like other WPA-enabled client devices.

Beginning in Privileged Exec mode, follow these steps to set up the repeater as a WPA client:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.
Step 3	ssid <i>ssid-string</i>	Create an SSID and enter SSID configuration mode for the new SSID. The SSID can consist of up to 32 alphanumeric characters. SSIDs are case sensitive.
Step 4	authentication open	Enable open authentication for the SSID.
Step 5	authentication key-management wpa	Enable WPA authenticated key management for the SSID.
Step 6	infrastructure ssid	Designate the SSID as the SSID that the repeater uses to associate to other access points.

	Command	Purpose
Step 7	wpa-psk { hex ascii } [0 7] <i>encryption-key</i>	Enter a pre-shared key for the repeater. Enter the key using either hexadecimal or ASCII characters. If you use hexadecimal, you must enter 64 hexadecimal characters to complete the 256-bit key. If you use ASCII, you must enter from 8 to 63 ASCII characters, and the access point expands the key for you.
Step 8	end	Return to privileged EXEC mode.
Step 9	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Understanding Hot Standby

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

Except for the IP address, the standby access point's settings should be identical to the settings on the monitored access point. If the monitored access point goes offline and the standby access point takes its place in the network, matching settings ensures that client devices can switch easily to the standby access point.

Hot standby mode is disabled by default.



Note

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



Note

The MAC address of the monitored access point might change if a BSSID on the monitored unit is added or deleted. If you use multiple BSSIDs on your wireless LAN, check the status of the standby unit when you add or delete BSSIDs on the monitored access point.

Configuring a Hot Standby Access Point

When you set up the standby access point, you must enter the MAC address of the access point that the standby unit will monitor. Record the MAC address of the monitored access point before you configure the standby access point.

The standby access point also must duplicate several key settings on the monitored access point. These settings are:

- Primary SSID (as well as additional SSIDs configured on the monitored access point)
- Default IP Subnet Mask

- Default Gateway
- Data rates
- WEP settings
- Authentication types and authentication servers

Check the monitored access point and record these settings before you set up the standby access point.

**Note**

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

**Tip**

To quickly duplicate the monitored access point's settings on the standby access point, save the monitored access point configuration and load it on the standby access point. See the [“Working with Configuration Files” section on page 18-8](#) for instructions on uploading and downloading configuration files.

Beginning in Privileged Exec mode, follow these steps to enable hot standby mode on an access point:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	iapp standby mac-address	Puts the access point into standby mode and specifies the MAC address of radio on the monitored access point. Note When you configure a 1200 Series access point with two radios to monitor a 1200 Series access point with two radios, you must enter the MAC addresses of both the monitored 2.4-GHz and 5-GHz radios. Enter the 2.4-GHz radio MAC address first, followed by the 5-GHz radio MAC address. Note The MAC address of the monitored access point might change if a BSSID on the monitored unit is added or deleted. If you use multiple BSSIDs on your wireless LAN, check the status of the standby unit when you add or delete BSSIDs on the monitored access point.
Step 3	interface dot11radio 0	Enter interface configuration mode for the radio interface.
Step 4	ssid ssid-string	Create the SSID that the standby access point uses to associate to the monitored access point; in the next step designate this SSID as an infrastructure SSID. If you created an infrastructure SSID on the monitored access point, create the same SSID on the standby access point, also.
Step 5	infrastructure-ssid [optional]	Designate the SSID as an infrastructure SSID. The standby uses this SSID to associate to the monitored access point. If the standby access point takes the place of the monitored access point, infrastructure devices must associate to the standby access point using this SSID unless you also enter the optional keyword.

	Command	Purpose
Step 6	authentication client username <i>username</i> password <i>password</i>	If the monitored access point is configured to require LEAP authentication, configure the username and password that the standby access point uses when it performs LEAP authentication. This username and password must match the username and password that you set up for the standby access point on the authentication server.
Step 7	exit	Exit SSID configuration mode and return to radio interface configuration mode.
Step 8	iapp standby poll-frequency <i>seconds</i>	Sets the number of seconds between queries that the standby access point sends to the monitored access point's radio and Ethernet ports. The default poll frequency is 2 seconds.
Step 9	iapp standby timeout <i>seconds</i>	Sets the number of seconds the standby access point waits for a response from the monitored access point before it assumes that the monitored access point has malfunctioned. The default timeout is 20 seconds. Note You should increase the standby timeout setting if the bridged path between the standby and monitored access points can be lost for periods greater than 20 seconds (during spanning tree recalculation, for example). Note If the monitored access point is configured to select the least congested radio channel, you might need to increase the standby timeout setting. The monitored unit might take up to 40 seconds to select the least congested channel.
Step 10	iapp standby primary-shutdown	(Optional) Configures the standby access point to send a Dumb Device Protocol (DDP) message to the monitored access point to disable the radios of the monitored access point when the standby unit becomes active. This feature prevents client devices that are associated to the monitored access point from remaining associated to the malfunctioning unit.
Step 11	show iapp standby-parms	Verify your entries. If the access point is in standby mode, this command displays the standby parameters, including the MAC address of the monitored access point and the poll-frequency and timeout values. If the access point is not in standby mode, <i>no iapp standby mac-address</i> appears.
Step 12	end	Return to privileged EXEC mode.
Step 13	copy running-config startup-config	(Optional) Save your entries in the configuration file.

After you enable standby mode, configure the settings that you recorded from the monitored access point to match on the standby access point.

Verifying Standby Operation

Use this command to check the status of the standby access point:

show iapp standby-status

This command displays the status of the standby access point. [Table 20-2](#) lists the standby status messages that can appear.

Table 20-2 Standby Status Messages

Message	Description
IAPP Standby is Disabled	The access point is not configured for standby mode.
IAPP—AP is in standby mode	The access point is in standby mode.
IAPP—AP is operating in active mode	The standby access point has taken over for the monitored access point and is functioning as a root access point.
IAPP—AP is operating in repeater mode	The standby access point has taken over for the monitored access point and is functioning as a repeater access point.
Standby status: Initializing	The standby access point is initializing link tests with the monitored access point.
Standby status: Takeover	The standby access point has transitioned to active mode.
Standby status: Stopped	Standby mode has been stopped by a configuration command.
Standby status: Ethernet Linktest Failed	An Ethernet link test failed from the standby access point to the monitored access point.
Standby status: Radio Linktest Failed	A radio link test failed from the standby access point to the monitored access point.
Standby status: Standby Error	An undefined error occurred.
Standby State: Init	The standby access point is initializing link tests with the monitored access point.
Standby State: Running	The standby access point is operating in standby mode and is running link tests to the monitored access point.
Standby State: Stopped	Standby mode has been stopped by a configuration command.
Standby State: Not Running	The access point is not in standby mode.

Use this command to check the standby configuration:

show iapp standby-parms

This command displays the MAC address of the standby access point, the standby timeout, and the poll-frequency values. If no standby access point is configured, this message appears:

```
no iapp standby mac-address
```

If a standby access point takes over for the monitored access point, you can use the **show iapp statistics** command to help determine the reason that the standby access point took over.

Understanding Workgroup Bridge Mode

You can configure the access point/bridge as a workgroup bridges. In workgroup bridge mode, the access point/bridge associates to another access point as a client and provides a network connection for the devices connected to its Ethernet port. For example, if you need to provide wireless connectivity for a group of network printers, you can connect the printers to a hub or to a switch, connect the hub or switch to the access point/bridge Ethernet port, and configure the access point/bridge as a workgroup bridge. The workgroup bridge associates to an access point on your network.

There is no limit on the number of devices that you can connect to the workgroup bridge's Ethernet port. However, the connected devices share the bandwidth provided by the link from the workgroup bridge to the root access point or bridge.

**Caution**

An access point/bridge in workgroup bridge mode can introduce a bridge loop if you connect its Ethernet port to your wired LAN. To avoid a bridge loop on your network, disconnect the workgroup bridge from your wired LAN before or soon after you configure it as a workgroup bridge.

**Note**

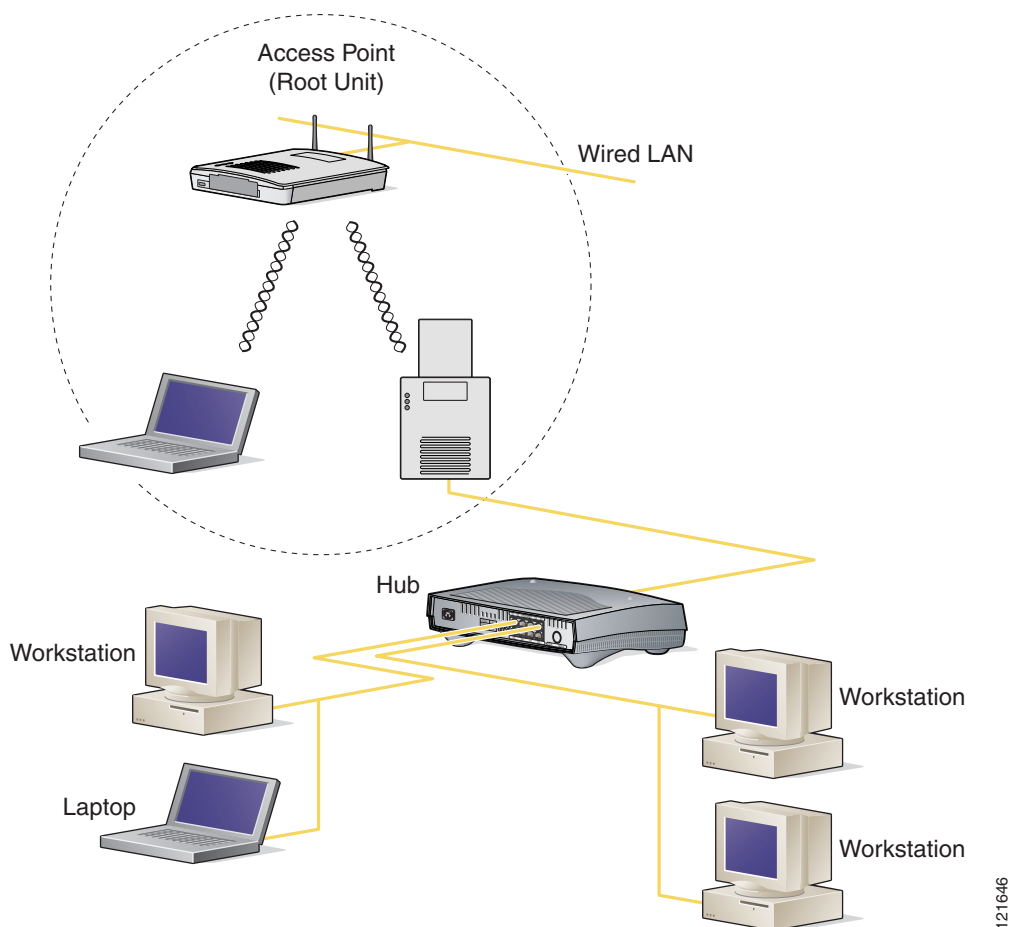
An access point/bridge in workgroup bridge mode can associate only to a Cisco Aironet access point or bridge.

**Note**

If multiple BSSIDs are configured on a root access point that is designated as the parent of a workgroup bridge, the parent MAC address might change if a BSSID on the parent is added or deleted. If you use multiple BSSIDs on your wireless LAN and a workgroup bridge on your wireless LAN is configured to associate to a specific parent, check the association status of the workgroup bridge when you add or delete BSSIDs on the parent access point.

Figure 20-2 shows an access point in workgroup bridge mode.

Figure 20-2 Access Point in Workgroup Bridge Mode



Treating Workgroup Bridges as Infrastructure Devices or as Client Devices

The access point to which a workgroup bridge associates can treat the workgroup bridge as an infrastructure device or as a simple client device. By default, access points and bridges treat workgroup bridges as client devices.

For increased reliability, you can configure access points and bridges to 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. You use the **infrastructure-client** configuration interface command to configure access points and bridges to treat workgroup bridges as infrastructure devices.

Configuring access points and bridges to treat a workgroup bridge as a client device allows more workgroup bridges to associate to the same access point, or to associate using an SSID that is not an infrastructure SSID. 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 an access point or bridge. 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. You use the **no infrastructure client** configuration interface command to configure access points and bridges to treat workgroup bridges as simple client devices. This is the default setting.

You should use a workgroup bridge as an infrastructure device if the devices connected to the workgroup bridge require network reliability equivalent to that of an access point or a bridge. You should use a workgroup bridge as a client device if these conditions are true:

- More than 20 workgroup bridges associate to the same access point or bridge
- The workgroup bridge associates using an SSID that is not an infrastructure SSID
- The workgroup bridge is mobile

Configuring a Workgroup Bridge for Roaming

If your workgroup bridge is mobile, you can configure it to scan for a better radio connection to a parent access point or bridge. Use this command to configure the workgroup bridge as a mobile station:

```
BR(config)# mobile station
```

When you enable this setting, the workgroup bridge scans for a new parent association when it encounters a poor Received Signal Strength Indicator (RSSI), excessive radio interference, or a high frame-loss percentage. Using these criteria, a workgroup bridge configured as a mobile station searches for a new parent association and roams to a new parent before it loses its current association. When the mobile station setting is disabled (the default setting) the workgroup bridge does not search for a new association until it loses its current association.

Configuring a Client VLAN

If the devices connected to the workgroup bridge's Ethernet port should all be assigned to a particular VLAN, you can configure a VLAN for the connected devices. Enter this command on the workgroup bridge:

```
ap(config)# workgroup-bridge client-vlan vlan-id
```

All the devices connected to the workgroup bridge's Ethernet port are assigned to that VLAN.

Configuring Workgroup Bridge Mode

Beginning in privileged EXEC mode, follow these steps to configure an access point/bridge as a workgroup bridge:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.

	Command	Purpose
Step 3	station-role workgroup-bridge	Set the radio role to workgroup bridge. If your access point contains two radios, the radio not set to workgroup bridge mode is automatically disabled.
Step 4	ssid <i>ssid-string</i>	Create the SSID that the workgroup bridge uses to associate to a parent access point or bridge.
Step 5	infrastructure-ssid	Designate the SSID as an infrastructure SSID. Note The workgroup bridge must use an infrastructure SSID to associate to a root access point or bridge.
Step 6	authentication client username <i>username</i> password <i>password</i>	(Optional) If the parent access point is configured to require LEAP authentication, configure the username and password that the workgroup bridge uses when it performs LEAP authentication. This username and password must match the username and password that you set up for the workgroup bridge on the authentication server.
Step 7	exit	Exit SSID configuration mode and return to radio interface configuration mode.
Step 8	parent {1-4} <i>mac-address</i> <i>[timeout]</i>	(Optional) Enter the MAC address for the access point to which the workgroup bridge should associate. - You can enter MAC addresses for up to four parent access points. The workgroup bridge attempts to associate to MAC address 1 first; if that access point does not respond, the workgroup bridge tries the next access point in its parent list. Note If multiple BSSIDs are configured on the parent access point, the MAC address for the parent might change if a BSSID on the parent is added or deleted. (Optional) You can also enter a timeout value in seconds that determines how long the workgroup bridge attempts to associate to a parent access point before trying the next parent in the list. Enter a timeout value from 0 to 65535 seconds.
Step 9	exit	Exit radio configuration mode and return to global configuration mode.
Step 10	workgroup-bridge client-vlan <i>vlan-id</i>	(Optional) Specify the VLAN to which the devices that are connected to the workgroup bridge's Ethernet port are assigned.
Step 11	mobile station	(Optional) Configure the workgroup bridge as a mobile station. When you enable this setting, the workgroup bridge scans for a new parent association when it encounters a poor Received Signal Strength Indicator (RSSI), excessive radio interference, or a high frame-loss percentage. When this setting is disabled (the default setting) the workgroup bridge does not search for a new association until it loses its current association.
Step 12	end	Return to privileged EXEC mode.
Step 13	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to configure an access point/bridge as a workgroup bridge. In this example, the workgroup bridge uses the configured username and password to perform LEAP authentication, and the devices attached to its Ethernet port are assigned to VLAN 22:

```
ap# configure terminal
ap(config)# interface dot11radio 0
ap(config-if)# station-role workgroup-bridge
ap(config-if)# ssid infra
ap(config-ssid)# infrastructure-ssid
ap(config-ssid)# authentication client username wgb1 password cisco123
ap(config-ssid)# exit
ap(config-if)# exit
ap(config)# workgroup-bridge client-vlan 22
ap(config)# end
```




Troubleshooting

This chapter provides troubleshooting procedures for basic problems with the access point/bridge. For the most up-to-date, detailed troubleshooting information, refer to the Cisco TAC website at the following URL (select **Hardware Support > Wireless Devices**):

<http://www.cisco.com/tac>

Sections in this chapter include:

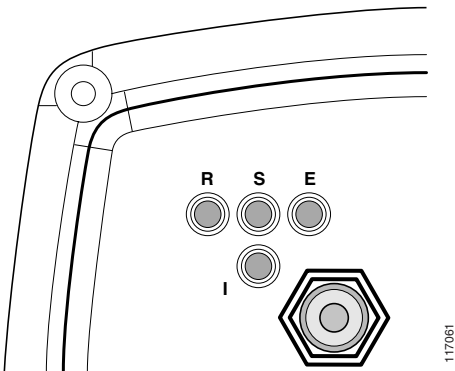
- [Checking the LEDs, page 21-2](#)
- [Power Injector, page 21-4](#)
- [Checking Power, page 21-5](#)
- [Checking Basic Configuration Settings, page 21-5](#)
- [Antenna Alignment, page 21-6](#)
- [Resetting the Access Point/Bridge to the Default Configuration, page 21-6](#)
- [Reloading the Access Point/Bridge Image, page 21-9](#)

Checking the LEDs

If your access point/bridge is not associating with a remote bridge or access point, check the four LEDs on the back panel. You can use them to quickly assess the unit’s status. For information on using the LEDs during the installation and alignment of the access point/bridge antenna, refer to the *Cisco Aironet 1300 Series Outdoor Access Point/Bridge Mounting Instructions* that shipped with your access point/bridge.

Figure 21-1 shows the access point/bridge LEDs.

Figure 21-1 LEDs



R	Radio LED	E	Ethernet LED
S	Status LED	I	Install LED

Normal Mode LED Indications

During access point/bridge operation the LEDs provide status information as shown in Table 21-1.

Table 21-1 LED Indications

Ethernet LED	Status LED	Radio LED	Install LED	Meaning
Off	—	—	—	Ethernet link is down or disabled.
Blinking green	—	—	—	Transmitting and receiving Ethernet packets.
Blinking amber	—	—	—	Transmitting and receiving Ethernet errors.
amber	—	—	—	Firmware error—disconnect and reconnect the power injector power jack. If the problem continues, contact technical support for assistance.

Table 21-1 LED Indications (continued)

Ethernet LED	Status LED	Radio LED	Install LED	Meaning
—	Blinking green	—	—	Root bridge mode—no remote bridges are associated. Non-root bridge mode—not associated to the root bridge. If all bridges are powered up, this could be caused by incorrect SSID and security settings or improper antenna alignment. You should check the SSID and security settings of all bridges and verify antenna alignment. If the problem continues, contact technical support for assistance.
—	Green	—	—	Root mode—associated to at least one remote bridge. Non-root mode—associated to the root bridge. This is normal operation.
—	Blinking amber	—	—	General warning—disconnect and reconnect the power injector power jack. If the problem continues, contact technical support for assistance.
—	Amber	—	—	Loading firmware.
Red	Amber	Red	—	Loading Firmware error—disconnect and reconnect the power injector power. If the problem continues, contact technical support for assistance.
—	—	Off	—	Normal operation.
—	—	Blinking green	—	Transmitting and receiving radio packets—normal operation.
—	—	Blinking amber	—	Maximum retries or buffer full occurred on the radio interface—disconnect and reconnect the power injector power jack. If the problem continues, contact technical support for assistance.
—	—	Amber	—	Radio firmware error—disconnect and reconnect power injector power. If the problem continues, contact technical support for assistance.
—	—	—	Amber blinking	Not associated (non-root mode). The access point/bridge attempts to associate with a root bridge for 60 seconds ¹ .
—	—	—	Amber	Associated (non-root mode).
—	—	—	Green blinking	Not associated (root mode). The access point/bridge attempts to associate with a non-root bridge indefinitely.
—	—	—	Green	Associated (root mode).
—	—	—	Red	Overcurrent or overvoltage error—disconnect power to the power injector, check all coax cable connections, wait approximately 1 minute, and reconnect power. If error continues, contact technical support.

1. Preconfigured bridges search indefinitely.

The access point/bridge uses a blinking code to identify various error conditions. The code sequence uses a two-digit diagnostic code that starts with a long pause to delimit the code, followed by the LED flashing red to count out the first digit, then a short pause, followed by the LED flashing red to count out the second digit.

The LED blinking error codes are described in [Table 21-2](#).

Table 21-2 LED Blinking Error Codes

LED	Blinking Codes		Description
	First Digit	Second Digit	
Ethernet	2	1	Ethernet cable problem—verify that the cable is properly connected and not defective. This error might also indicate a problem with the Ethernet link. If the cable is connected properly and not defective, contact technical support for assistance.
Radio	1	2	Radio not detected—contact technical support for assistance.
	1	3	Radio not ready—contact technical support for assistance.
	1	4	Radio did not start—contact technical support for assistance.
	1	5	Radio failure—contact technical support for assistance.
	1	6	Radio did not flash its firmware—contact technical support for assistance.

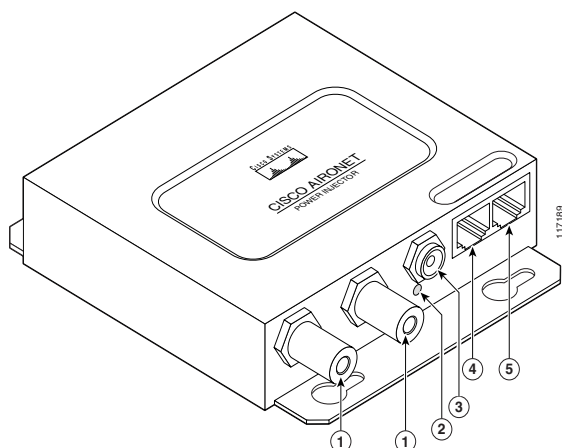
Power Injector

When the power injector is powered up, it applies 48-VDC to the dual-coax cables to the access point/bridge.

When power is applied to the access point/bridge, the unit activates the bootloader and begins the POST operations. The access point/bridge begins to load the IOS image when the Post operations are successfully completed. Upon successfully loading the IOS image, the unit initializes and tests the radio.

The power injector LED is shown in [Figure 21-2](#).

Figure 21-2 Power Injector



1	Dual-coax Ethernet ports (F-Type connectors)	4	Ethernet LAN port (RJ-45 connector)
2	Power LED	5	Console serial port (RJ-45 connector)
3	Power jack		

The power injector is available in two models:

- Cisco Aironet Power Injector LR2—standard version (included with the bridge)
 - 48-VDC input power
 - Uses the 48-VDC power module (included with the bridge)
- Cisco Aironet Power Injector LR2T—optional transportation version
 - 12- to 40-VDC input power
 - Uses 12 to 40 VDC from a vehicle battery

Checking Power

You can verify the availability of power to the access point/bridge by checking the power injector LED (see [Figure 21-2](#)):

- Power LED
 - Green color indicates input power is being supplied to the bridge.
 - Red color indicates an overcurrent or overvoltage error condition—disconnect input power from the power injector, check all coax cable connections for a possible short, wait approximately 1 minute, and reconnect input power to the power injector. If the LED turns red again, contact technical support for assistance.



Note The power injector requires approximately 50 seconds to recover from an overcurrent or overvoltage condition.

- Off indicates input power is not available—verify that the power module is connected to the power injector and that AC power is available or that 12- to 40-VDC input power is connected to the power injector.

Checking Basic Configuration Settings

Mismatched basic settings are the most common causes of lost wireless connectivity. If the access point/bridge does not associate with a remote bridge, access point, or client device, check the following areas.

SSID

Wireless clients attempting to associate with the bridge must use the same SSID as the bridge. If a client device's SSID does not match the SSID of an bridge in radio range, the client device will not associate.



Note

Access points and bridges are not designed to associate together. However, a workgroup bridge can associate to either a Cisco Aironet access point or a Cisco Aironet bridge.

WEP Keys

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

Refer to [Chapter 9, “Configuring Cipher Suites and WEP,”](#) for instructions on setting the wireless device’s WEP keys.

Security Settings

Wireless clients attempting to authenticate with the bridge must support the same security options configured in the access point/bridge, such as EAP or LEAP, MAC address authentication, Message Integrity Check (MIC), WEP key hashing, and 802.1X protocol versions.

If a wireless client is unable to authenticate with the access point/bridge, contact the system administrator for proper security settings in the client adapter and for the client adapter driver and firmware versions that are compatible with the access point/bridge settings.

**Note**

The access point/bridge MAC address that appears on the Status page in the Aironet Client Utility (ACU) is the MAC address for the bridge radio. The MAC address for the access point Ethernet port is printed on the label on the back of the access point.

Antenna Alignment

If your non-root bridges or non-root access points are unable to associate to your root bridge or root access point, you should verify the basic configuration settings on all bridges or access points before attempting to verify antenna alignment ([Chapter 2, “Configuring the Access Point/Bridge for the First Time.”](#) If your basic configuration settings are correct, you can verify antenna alignment by using the Install mode RSSI LED indications. For additional information, refer to the *Cisco Aironet 1300 Series Outdoor Access Point/Bridge Mounting Instructions* that shipped with your access point/bridge.

**Note**

To meet regulatory restrictions, the external antenna access point/bridge unit and the external antenna must be professionally installed. The network administration or other IT professional responsible for installing and configuring the unit is a suitable professional installer. Following installation, access to the unit should be password protected by the network administrator to maintain regulatory compliance.

Resetting the Access Point/Bridge to the Default Configuration

You can use the web-browser interface or the CLI to reset the access point/bridge to a factory default configuration.

**Note**

The following steps reset *all* configuration settings to factory defaults, including passwords, WEP keys, the IP address, and the SSID. The default username and password are both **Cisco**, which is case-sensitive.

Using the Web-Browser Interface

Follow the steps below to delete the current configuration and return all access point/bridge settings to the factory defaults using the Web-browser interface.

-
- Step 1** Open your Internet browser.
- Step 2** Enter the bridge's IP address in the browser address or location line and press **Enter**. An Enter Network Password screen appears.
- Step 3** Enter your username (default *Cisco*) in the User Name field.
- Step 4** Enter the access point/bridge password (default *Cisco*) in the Password field and press **Enter**. The Summary Status page appears.
- Step 5** Click **System Software** and the System Software screen appears.
- Step 6** Click **System Configuration** and the System Configuration screen appears.
- Step 7** Click one of the following:
- a. **Reset to Defaults**. This option deletes a static IP address and resets the Configuration Server Protocol setting to DHCP.
 - b. **Reset to Defaults (Except IP)**. This option does not reset the IP address.
- Step 8** After the access point/bridge reboots, you can reconfigure the access point/bridge by using the Web-browser interface or the CLI (refer to the *Cisco IOS Software Configuration Guide for Cisco Aironet Bridges* or to the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*).
-

Using the CLI

From the privileged EXEC mode, you can reset the access point/bridge configuration to factory default values using the CLI by following these steps:

-
- Step 1** Enter **erase nvram:** to erase all NVRAM files including the startup configuration.
- Step 2** Enter **Y** when the following CLI message displays: *Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]*.
- Step 3** Enter **reload** when the following CLI message displays: *Erase of nvram: complete*. This command reloads the operating system.
- Step 4** Enter **Y** when the following CLI message displays: *Proceed with reload? [confirm]*.

**Caution**

Do not interrupt the boot process to avoid damaging the configuration file. Wait until the access point/bridge Install Mode LED begins to blink green before continuing with CLI configuration changes. You can also see the following CLI message when the load process has finished: *Line protocol on Interface Dot11Radio0, changed state to up.*

Step 5

After the access point/bridge reboots, you can reconfigure the access point/bridge by using the Web-browser interface or the CLI (refer to the *Cisco IOS Software Configuration Guide for Cisco Aironet Bridges* or to the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*). The access point/bridge is configured with the factory default values including the IP address (set to receive an IP address using DHCP). To obtain the unit's new IP address, you can use the *show interface bvi1* CLI command. If the unit does not receive an IP address from a DHCP server, the access point/bridge IP address is 10.0.0.1.

Corrupt IOS Configuration or Lost Password Procedure

This section describes the procedure for resetting the access point/bridge to its default settings in the unlikely event that the operating system is corrupt or if you have misplaced the configuration login and password. Because the access point/bridge does not have a mode switch, you must use the console port to perform this operation. Follow these steps to reset the unit to its default settings:

Step 1

Open the CLI using a Telnet session or a connection to the access point/bridge's console port.

Step 2

Reboot the access point/bridge by removing power and reapplying power.

Step 3

Let the access point/bridge boot until the command prompt appears and the access point/bridge begins to inflate the image. When you see these lines on the CLI, press **Esc**:

**Note**

Depending on the terminal emulation software you are using, you may have to press **Esc** twice to access the boot loader.

```
Loading "flash:/c1310-k9kw-7mx.v122_15_ja.200040314-k9w7-mx.v122_15_ja.20040314"
...#####
#####
#####
```

Messages similar to those below appear:

```
Error loading "flash:/c1310-k9kw-7mx.v122_15_ja.200040314-k9w7-mx.v122_15_ja.20040314"
```

```
Interrupt within 5 seconds to abort boot process.
Boot process terminated.
```

```
The system is unable to boot automatically. The BOOT environment variable needs to be set
to a bootable image.
```

```
C1310 Boot Loader (C1310-BOOT-M), Version 12.2 [BLD-v122_15_ja_throttle.20040314 100]
```

```
ap:
```

Step 4

At the prompt, enter the following command to show a directory of the flash file system similar to the directory shown below:


```

ap: dir flash:
Directory of flash:/

 2  -rwx   0      <date>    env_vars
 5  drwx  384    <date>    C1310-k9w7-mx.v133_15_JA.20040314
 3  -rwx  1128   <date>    config.txt
 4  -rwx   5      <date>    private-config

3693568 bytes available (4047872 bytes used)

```

Step 5 Reboot the bridge.



Note

The access point/bridge is configured with factory default values, including the IP address (set to receive an IP address using DHCP) and the default case-sensitive user name and password (**Cisco**).



Note

If your access point/bridge does not use a DHCP server to obtain an IP address, it continues to request a DHCP address. To assign an IP address, you must access the CLI using the console. See [“Obtaining and Assigning an IP Address” section on page 2-2](#) for information.

Reloading the Access Point/Bridge Image

If your access point/bridge has a firmware failure, you must reload the complete image file using the Web-browser interface or by using the console serial port. You can use the browser interface if the access point/bridge firmware is operational. However, you can use the console serial port when the access point/bridge has a corrupt image.

Web-Browser Interface

You can also use the Web-browser interface to reload the access point/bridge image file. The Web-browser interface supports loading the image file using HTTP or TFTP interfaces.



Note

Your access point/bridge configuration is not changed when using the browser to reload the image file.

Browser HTTP Interface

The HTTP interface enables you to browse to the access point/bridge image file on your PC and download the image to the unit. Follow the instructions below to use the HTTP interface:

- Step 1** Open your Internet browser.
- Step 2** Enter the access point/bridge's IP address in the browser address or location line and press **Enter**. An Enter Network Password screen appears.

- Step 3** Enter your username in the User Name field.
 - Step 4** Enter the access point/bridge password in the Password field and press **Enter**. The Summary Status page appears.
 - Step 5** Click the **System Software** tab and then click **Software Upgrade**. The HTTP Upgrade screen appears.
 - Step 6** Click **Browse** to locate the image file on your PC.
 - Step 7** Click **Upgrade**.
 - Step 8** After the access point/bridge reboots, you can reconfigure the unit by using the Web-browser interface or the CLI (refer to the *Cisco IOS Software Configuration Guide for Cisco Aironet Bridges* or to the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*).
For additional information, click the **Help** icon on the Software Upgrade screen.
-

Browser TFTP Interface

The TFTP interface enables you to use a TFTP server on a network device to load the access point/bridge image file. Follow the instructions below to use a TFTP server:

-
- Step 1** Open your Internet browser.
 - Step 2** Enter the access point/bridge's IP address in the browser address or location line and press **Enter**. An Enter Network Password screen appears.
 - Step 3** Enter your username in the User Name field.
 - Step 4** Enter the access point/bridge password in the Password field and press **Enter**. The Summary Status page appears.
 - Step 5** Click **System Software** and then click **Software Upgrade**. The HTTP Upgrade screen appears.
 - Step 6** Click **TFTP Upgrade**. The TFTP Upgrade screen appears.
 - Step 7** Enter the IP address for the TFTP file server in the TFTP File Server field.
 - Step 8** Enter the filename for the access point/bridge image file (*c1310-k9w7-tar.122-15.JA.tar*) in the Upload New System Image Tar File field. If the file is located in a subdirectory of the TFTP server root directory, include the relative path of the TFTP server root directory with the filename. If the file is in the TFTP root directory, enter only the filename.
 - Step 9** Click **Upgrade**.
 - Step 10** After the access point/bridge reboots, you can reconfigure the access point/bridge by using the Web-browser interface or the CLI (refer to the *Cisco IOS Software Configuration Guide for Cisco Aironet Bridges* or to the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*).
For additional information click the **Help** icon on the Software Upgrade screen.
-

Using the CLI

Follow the steps below to reload the access point image using the CLI. When the access point begins to boot, you interrupt the boot process and use boot loader commands to load an image from a TFTP server to replace the image in the access point.



Note Your access point configuration is not changed when using the CLI to reload the image file.

- Step 1** Open the CLI using a Telnet session or a connection to the access point console port.
- Step 2** Reboot the access point by removing power and reapplying power.
- Step 3** Let the access point boot until it begins to inflate the image. When you see these lines on the CLI, press **Esc**:

```
Loading "flash:/c1310-k9w7-mx.v122_13_ja.20031010/c1310-k9w7-mx.v122_13_ja.20031010"
...#####
#####
#####
#####
#####
```



Note Depending on the terminal emulation software you are using, you may have to press **Esc** twice to access the boot loader.

- Step 4** When the bridge: command prompt appears, enter the **set** command to assign an IP address, subnet mask, and default gateway to the access point.



Note You must use upper-case characters when you enter the **IP-ADDR**, **NETMASK**, and **DEFAULT_ROUTER** options with the **set** command.

Your entries might look like this example:

```
ap: set IP_ADDR 192.168.133.160
ap: set NETMASK 255.255.255.0
ap: set DEFAULT_ROUTER 192.168.133.1
```

- Step 5** Enter the **tftp_init** command to prepare the access point for TFTP.
- ```
ap: tftp_init
```
- Step 6** Enter the **tar** command to load and inflate the new image from your TFTP server. The command must include this information:
- the **-xtract** option, which inflates the image when it is loaded
  - the IP address of your TFTP server
  - the directory on the TFTP server that contains the image
  - the name of the image
  - the destination for the image (the access point Flash)

Your entry might look like this example:

```
ap: tar -xtract tftp://192.168.130.222/images/c1310-k9w7-tar.122_15.JA1 flash:
```

- Step 7** When the display becomes full the CLI pauses and displays **--MORE--**. Press the spacebar to continue.

```
extracting info (229 bytes)
c1310-k9w7-mx.122-15.JA1/ (directory) 0 (bytes)
c1310-k9w7-mx.122-15.JA1/html/ (directory) 0 (bytes)
c1310-k9w7-mx.122-15.JA1/html/level1/ (directory) 0 (bytes)
extracting c1310-k9w7-mx.122-15.JA1/html/level1/appsu.js (558 bytes)
extracting c1310-k9w7-mx.122-15.JA1/html/level1/back.htm (205 bytes)
```

```

extracting c1310-k9w7-mx.122-15.JA1/html/level1/cookies.js (5027 bytes).
extracting c1310-k9w7-mx.122-15.JA1/html/level1/forms.js (15704 bytes)...
extracting c1310-k9w7-mx.122-15.JA1/html/level1/sitewide.js (14621 bytes)...
extracting c1310-k9w7-mx.122-15.JA1/html/level1/config.js (2554 bytes)
extracting c1310-k9w7-mx.122-15.JA1/html/level1/styleSheet.css (3215 bytes)
c1310-k9w7-mx.122-15.JA1/html/level1/images/ (directory) 0 (bytes)
extracting c1310-k9w7-mx.122-15.JA1/html/level1/images/ap_title_appname.gif (1422 bytes)
extracting c1310-k9w7-mx.122-15.JA1/html/level1/images/apps_button_1st.gif (1171 bytes)
extracting c1310-k9w7-mx.122-15.JA1/html/level1/images/apps_button_cbottom.gif (318 bytes)
extracting c1310-k9w7-mx.122-15.JA1/html/level1/images/apps_button_current.gif (348 bytes)
extracting c1310-k9w7-mx.122-15.JA1/html/level1/images/apps_button_last.gif (386 bytes)
extracting c1310-k9w7-mx.122-15.JA1/html/level1/images/apps_button_last_filler.gif (327
bytes)
extracting c1310-k9w7-mx.122-15.JA1/html/level1/images/apps_button_last_flat.gif (318
bytes)
extracting c1310-k9w7-mx.122-15.JA1/html/level1/images/apps_button_nth.gif (1177 bytes)
extracting c1310-k9w7-mx.122-15.JA1/html/level1/images/apps_leftnav_dkgreen.gif (869
bytes)
-- MORE --

```

If you do not press the spacebar to continue, the process eventually times out and the access point stops inflating the image.

- Step 8** Enter the **set BOOT** command to designate the new image as the image that the access point uses when it reboots. The access point creates a directory for the image that has the same name as the image, and you must include the directory in the command. Your entry might look like this example:

```
ap: set BOOT flash:/c1310-k9w7-mx.122-15.JA1/c1310-k9w7-mx.122-15.JA1
```

- Step 9** Enter the **set** command to check your bootloader entries.

```

ap: set
BOOT=flash:/c1310-k9w7-mx.122-15.JA1/c1310-k9w7-mx.122-15.JA1
DEFAULT_ROUTER=192.168.133.1
IP_ADDR=192.168.133.160
NETMASK=255.255.255.0

```

- Step 10** Enter the **boot** command to reboot the access point. When the access point reboots, it loads the new image.

```
ap: boot
```

## Obtaining the Access Point/Bridge Image File

You can obtain the access point/bridge image file from the Cisco.com software center by following these steps:

- Step 1** Use your Web-browser to go to the Cisco Software Center at the following URL:  
<http://www.cisco.com/cisco/software/navigator.html>
- Step 2** Select **Option #1: Aironet Wireless Software Display Tables**. The Wireless Software page appears.
- Step 3** Scroll down to the Cisco Aironet Wireless Bridge Firmware and Utilities section and click **Cisco Aironet 1300 Series**. The Software Download page for the Cisco Aironet 1300 Series Wireless Bridge Firmware and Utilities appears.
- Step 4** Select the release you desire to download and click **Submit**. The Encryption Authorization Form appears.

- Step 5** On the Encryption Authorization Form, enter the requested information, read the encryption information, and check the boxes that apply. Click **Submit**.
  - Step 6** Read and accept the terms and conditions of the Software License Agreement.
  - Step 7** Select the access point/bridge image file again to download it.
  - Step 8** Save the file to a directory on your hard drive and then exit the Internet browser.
- 

## Obtaining the TFTP Server Software

You can download TFTP server software from several web sites. Cisco recommends the shareware TFTP utility available at this URL:

<http://tftpd32.jounin.net>

Follow the instructions on the website for installing and using the utility.





## Protocol Filters

---

The tables in this appendix list some of the protocols that you can filter on the access point/bridge. The tables include:

- Table E-1, [Ethernet Protocols](#)
- Table E-2, [IP Protocols](#)
- Table E-3, [IP Port Protocols](#)

In each table, the Protocol column lists the protocol name, the Additional Identifier column lists other names for the same protocol, and the ISO Designator column lists the numeric designator for each protocol.

**Table A-1**      **Ethertype Protocols**

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



**Table A-2**      *IP Protocols*

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

**Table A-3 IP Port Protocols**

| Protocol                       | Additional Identifier | ISO Designator |
|--------------------------------|-----------------------|----------------|
| TCP port service multiplexer   | tcpmux                | 1              |
| echo                           | —                     | 7              |
| discard (9)                    | —                     | 9              |
| systat (11)                    | —                     | 11             |
| daytime (13)                   | —                     | 13             |
| netstat (15)                   | —                     | 15             |
| Quote of the Day               | qotd<br>quote         | 17             |
| Message Send Protocol          | msp                   | 18             |
| ttytst source                  | chargen               | 19             |
| FTP Data                       | ftp-data              | 20             |
| FTP Control (21)               | ftp                   | 21             |
| Secure Shell (22)              | ssh                   | 22             |
| Telnet                         | —                     | 23             |
| Simple Mail Transport Protocol | SMTP<br>mail          | 25             |
| time                           | timserver             | 37             |
| Resource Location Protocol     | RLP                   | 39             |
| IEN 116 Name Server            | name                  | 42             |
| whois                          | nickname<br>43        | 43             |
| Domain Name Server             | DNS<br>domain         | 53             |
| MTP                            | —                     | 57             |
| BOOTP Server                   | —                     | 67             |
| BOOTP Client                   | —                     | 68             |
| TFTP                           | —                     | 69             |
| gopher                         | —                     | 70             |
| rje                            | netrjs                | 77             |
| finger                         | —                     | 79             |
| Hypertext Transport Protocol   | HTTP<br>www           | 80             |
| ttylink                        | link                  | 87             |
| Kerberos v5                    | Kerberos<br>krb5      | 88             |
| supdup                         | —                     | 95             |
| hostname                       | hostnames             | 101            |

**Table A-3** *IP Port Protocols (continued)*

| <b>Protocol</b>                    | <b>Additional Identifier</b>                   | <b>ISO Designator</b> |
|------------------------------------|------------------------------------------------|-----------------------|
| TSAP                               | iso-tsap                                       | 102                   |
| CSO Name Server                    | cso-ns<br>csnet-ns                             | 105                   |
| Remote Telnet                      | rtelnet                                        | 107                   |
| Postoffice v2                      | POP2<br>POP v2                                 | 109                   |
| Postoffice v3                      | POP3<br>POP v3                                 | 110                   |
| Sun RPC                            | sunrpc                                         | 111                   |
| tap ident authentication           | auth                                           | 113                   |
| sftp                               | —                                              | 115                   |
| uucp-path                          | —                                              | 117                   |
| Network News Transfer Protocol     | Network News<br>readnews<br>nntp               | 119                   |
| USENET News Transfer Protocol      | Network News<br>readnews<br>nntp               | 119                   |
| Network Time Protocol              | ntp                                            | 123                   |
| NETBIOS Name Service               | netbios-ns                                     | 137                   |
| NETBIOS Datagram Service           | netbios-dgm                                    | 138                   |
| NETBIOS Session Service            | netbios-ssn                                    | 139                   |
| Interim Mail Access Protocol v2    | Interim Mail<br>Access Protocol<br>IMAP2       | 143                   |
| Simple Network Management Protocol | SNMP                                           | 161                   |
| SNMP Traps                         | snmp-trap                                      | 162                   |
| ISO CMIP Management Over IP        | CMIP Management<br>Over IP<br>cmip-man<br>CMOT | 163                   |
| ISO CMIP Agent Over IP             | cmip-agent                                     | 164                   |
| X Display Manager Control Protocol | xdmcp                                          | 177                   |
| NeXTStep Window Server             | NeXTStep                                       | 178                   |
| Border Gateway Protocol            | BGP                                            | 179                   |
| Prospero                           | —                                              | 191                   |
| Internet Relay Chap                | IRC                                            | 194                   |

**Table A-3** *IP Port Protocols (continued)*

| Protocol                            | Additional Identifier | ISO Designator |
|-------------------------------------|-----------------------|----------------|
| SNMP Unix Multiplexer               | smux                  | 199            |
| AppleTalk Routing                   | at-rtmp               | 201            |
| AppleTalk name binding              | at-nbp                | 202            |
| AppleTalk echo                      | at-echo               | 204            |
| AppleTalk Zone Information          | at-zis                | 206            |
| NISO Z39.50 database                | z3950                 | 210            |
| IPX                                 | —                     | 213            |
| Interactive Mail Access Protocol v3 | imap3                 | 220            |
| Unix Listserv                       | ulistserv             | 372            |
| syslog                              | —                     | 514            |
| Unix spooler                        | spooler               | 515            |
| talk                                | —                     | 517            |
| ntalk                               | —                     | 518            |
| route                               | RIP                   | 520            |
| timeserver                          | timed                 | 525            |
| newdate                             | tempo                 | 526            |
| courier                             | RPC                   | 530            |
| conference                          | chat                  | 531            |
| netnews                             | —                     | 532            |
| netwall                             | wall                  | 533            |
| UUCP Daemon                         | UUCP<br>uucpd         | 540            |
| Kerberos rlogin                     | klogin                | 543            |
| Kerberos rsh                        | kshell                | 544            |
| rfs_server                          | remotefs              | 556            |
| Kerberos kadmin                     | kerberos-adm          | 749            |
| network dictionary                  | webster               | 765            |
| SUP server                          | supfilesrv            | 871            |
| swat for SAMBA                      | swat                  | 901            |
| SUP debugging                       | supfiledbg            | 1127           |
| ingreslock                          | —                     | 1524           |
| Prospero non-privileged             | prospero-np           | 1525           |
| RADIUS                              | —                     | 1812           |
| Concurrent Versions System          | CVS                   | 2401           |
| Cisco IAPP                          | —                     | 2887           |
| Radio Free Ethernet                 | RFE                   | 5002           |



## Supported MIBs

---

This appendix lists the Simple Network Management Protocol (SNMP) Management Information Bases (MIBs) that the access point/bridge supports for this software release. The Cisco IOS SNMP agent supports both SNMPv1 and SNMPv2. This appendix contains these sections:

- [MIB List, page B-1](#)
- [Using FTP to Access the MIB Files, page B-2](#)

### MIB List

- IEEE802dot11-MIB
- Q-BRIDGE-MIB
- P-BRIDGE-MIB
- CISCO-DOT11-IF-MIB
- CISCO-WLAN-VLAN-MIB
- CISCO-IETF-DOT11-QOS-MIB
- CISCO-IETF-DOT11-QOS-EXT-MIB
- CISCO-DOT11-ASSOCIATION-MIB
- CISCO-L2-DEV-MONITORING-MIB
- CISCO-DDP-IAPP-MIB
- CISCO-IP-PROTOCOL-FILTER-MIB
- CISCO-SYSLOG-EVENT-EXT-MIB
- CISCO-TBRIDGE-DEV-IF-MIB
- BRIDGE-MIB
- CISCO-CDP-MIB
- CISCO-CONFIG-COPY-MIB
- CISCO-CONFIG-MAN-MIB
- CISCO-FLASH-MIB
- CISCO-IMAGE-MIB
- CISCO-MEMORY-POOL-MIB

- CISCO-PROCESS-MIB
- CISCO-PRODUCTS-MIB
- CISCO-SMI-MIB
- CISCO-TC-MIB
- CISCO-SYSLOG-MIB
- ENTITY-MIB
- IF-MIB
- OLD-CISCO-CHASSIS-MIB
- OLD-CISCO-SYS-MIB
- OLD-CISCO-SYSTEM-MIB
- OLD-CISCO-TS-MIB
- RFC1213-MIB
- RFC1398-MIB
- SNMPv2-MIB
- SNMPv2-SMI
- SNMPv2-TC

## Using FTP to Access the MIB Files

Follow these steps to obtain each MIB file by using FTP:

- 
- Step 1** Use FTP to access the server **ftp.cisco.com**.
- Step 2** Log in with the username **anonymous**.
- Step 3** Enter your e-mail username when prompted for the password.
- Step 4** At the `ftp>` prompt, change directories to **/pub/mibs/v1** or **/pub/mibs/v2**.
- Step 5** Use the **get *MIB\_filename*** command to obtain a copy of the MIB file.
- 



**Note**

You can also access information about MIBs on the Cisco web site:  
<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

---



# Error and Event Messages

This appendix lists the CLI error and event messages.

## Conventions

System error messages are displayed in the format shown in [Table C-1](#).

**Table C-1**      **System Error Message Format**

| Message Component  | Description                                               | Example                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------|-----------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Error identifier   | A string categorizing the error.                          | STATION_ROLE                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Software component | A string identifying the software component of the error. | AUTO_INSTALL                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Severity Level     | A string indicating the severity of the error.            | LOG_DEBUG—debug information (not serious)<br>LOG_INFO—informational (not serious)<br>LOG_NOTICE—notice that may be of concern to user<br>LOG_WARNING—warning that user can ignore if they prefer<br>LOG_ERR—warning of error condition, most features functional; user should exercise care<br>LOG_CRIT—warns of a possible serious critical error<br>LOG_ALERT—alerts user to a very serious problem<br>LOG_EMERG—emergency situation, nothing is functional |

**Table C-1** System Error Message Format (continued)

| Message Component | Description                                                    | Example                                                                                                                                                                                                                                                              |
|-------------------|----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Action Flags      | Internal to the code for which additional action is displayed. | 0—No action flag<br>MSG_TRACEBACK—includes traceback with message<br>MSG_PROCESS—includes process information with message<br>MSG_CLEAR—indicates condition had cleared<br>MSG_SECURITY—indicates as security message<br>MSG_NOSCAN—suppresses EEM pattern screening |
| %d                | An integer number.                                             | 2450                                                                                                                                                                                                                                                                 |
| %e                | A MAC address.                                                 | 000b.fcff.b04e                                                                                                                                                                                                                                                       |
| %s                | A message string which provides more detail of the error.      | “Attempt to protect port 1640 failed.”                                                                                                                                                                                                                               |
| %x                | A hexadecimal number.                                          | 0x001                                                                                                                                                                                                                                                                |

## Software Auto Upgrade Messages

**Error Message** FATAL\_FAILURE, SW\_AUTO\_UPGRADE, LOG\_CRIT, MSG\_PROCESS: “Attempt to upgrade software failed, software on flash may be deleted. Please copy software into flash.”

**Explanation** Auto upgrade of the software failed. The software on the flash might have been deleted. Copy software into the flash.

**Recommended Action** Copy software before rebooting the unit.

**Error Message** DHCP\_CLIENT\_FAILURE, SW\_AUTO\_UPGRADE, LOG\_DEBUG, MSG\_TRACEBACK | MSG\_PROCESS, “%s”: Auto upgrade of the software failed.”

**Explanation** Auto upgrade of the software failed.

**Recommended Action** Make sure that the DHCP client is running.

**Error Message** DHCP\_SERVER\_FAILURE, SW\_AUTO\_UPGRADE, LOG\_DEBUG, MSG\_TRACEBACK | MSG\_PROCESS, “%s”: Auto upgrade of the software failed.”

**Explanation** Auto upgrade of the software failed.

**Recommended Action** Make sure that the DHCP server is configured correctly.



**Error Message** BOOT\_FAILURE, SW\_AUTO\_UPGRADE, LOG\_DEBUG, MSG\_TRACEBACK, MSG\_PROCESS, "%s": Auto upgrade of the software failed."

**Explanation** Auto upgrade of the software failed.

**Recommended Action** Reboot the unit. If the message appears again, copy the error message exactly as it appears and report it to your technical support representative.

**Error Message** STATION\_ROLE, AUTO\_INSTALL, LOG\_WARNING, 0, "%s": The radio is operating in automatic install mode."

**Explanation** The radio is operating in automatic install mode.

**Recommended Action** Use the **station-role** configuration interface command to configure the radio for a role other than install mode.

**Error Message** IP\_ADDRESS\_DHCP, AUTO\_INSTALL, LOG\_WARNING, 0: "The radio is operating in automatic install mode and has set ip address dhcp."

**Explanation** The radio is operating in automatic install mode and is configured to receive an IP address through DHCP.

**Recommended Action** Use the **station-role** configuration interface command to configure the radio for a role other than install mode.

**Error Message** STATUS\_AUTO\_INSTALL, LOG\_INFO, 0, "%s" %s. RSSI=-%d dBm.: The radio is operating in install mode."

**Explanation** The radio is operating in automatic install mode.

**Recommended Action** Use the **station-role** configuration interface command to configure the radio for a role other than install mode.

## Association Management Messages

**Error Message** BADSTATE, DOT11, LOG\_ERR, 0, "%s %s ->%s."

**Explanation** 802.11 association and management uses a table-driven state machine to keep track and transition an association through various states. A state transition occurs when an association receives one of many possible events. When this error occurs, it means that an association received an event that it did not expect while in this state.

**Recommended Action** The system can continue but may lose the association that generates this error. Copy the message exactly as it appears and report it to your technical service representative.

**Error Message** ASSOC, DOT11, LOG\_INFO, 0, "Interface %s, Station %s e% %s KEY\_MGMT (%s)."

**Explanation** The indicated station associated to an access point on the indicated interface.

**Recommended Action** None.

**Error Message** ADD, DOT11, LOG\_INFO, 0 "Interface %s, Station %e associated to parent %e."

**Explanation** The indicated station associated to the parent access point on the indicated interface.

**Recommended Action** None.

**Error Message** DISASSOC, DOT11, LOG\_INFO, 0, "Interface %s, Deauthenticating Station %e %s."

**Explanation** The indicated station disassociated from the access point on the indicated interface.

**Recommended Action** None.

**Error Message** ROAMED, DOT11, LOG\_INFO, 0, "Station %e roamed to %e."

**Explanation** The indicated station roamed to the indicated new access point.

**Recommended Action** None.

**Error Message** ENCRYPT\_MISMATCH, DOT11, LOG\_WARNING, 0, "Possible encryption key mismatch between interface %s and station %e."

**Explanation** The encryption setting of the indicated interface and indicated station may be mismatched.

**Recommended Action** Check the encryption configuration of this interface and the failing station to ensure that the configurations match.

## Unzip Messages

**Error Message** UNZIP\_OVERFLOW, SOAP, LOG\_WARNING, MSG\_TRACEBACK: "Failed to unzip %s, exceeds maximum uncompressed html size."

**Explanation** The HTTP server cannot retrieve a compressed file in response to an HTTP GET request because the file is too large for the buffers used in the uncompression process.

**Recommended Action** Make sure that the file is a valid HTML page. If it is, you need to copy an uncompressed version of the file into Flash to retrieve it through HTTP.

## 802.11 Subsystem Messages

**Error Message** `FREQ_USED, DOT11, LOG_INFO, 0 "Interface %s, frequency %d selected."`

**Explanation** After scanning for an unused frequency, the indicated interface selected the displayed frequency.

**Recommended Action** None.

**Error Message** `NO_VALID_INFRA_SSID, DOT11, LOG_WARNING, 0, "No infrastructure SSID configured. %s not started."`

**Explanation** No infrastructure SSID was configured and the indicated interface was not started.

**Recommended Action** Add at least one infrastructure SSID to the radio configuration.

**Error Message** `VERSION_UPGRADE, DOT11, LOG_WARNING, 0, "Interface %d, upgrading radio firmware."`

**Explanation** When starting the indicated interface, the access point found the wrong firmware version. The radio will be loaded with the required version.

**Recommended Action** None.

**Error Message** `VERSION_INVALID, DOT11, LOG_CRIT, 0, "Interface %d, unable to find required radio version %x.%x/ %d/`

**Explanation** When trying to re-flash the radio firmware on the indicated interface, the access point recognized that the indicated radio firmware packaged with the Cisco IOS software had the incorrect version.

**Recommended Action** None.

**Error Message** `RADIO_OVER_TEMPERATURE, DOT11, LOG_ERR, 0, "Interface %s Radio over temperature detected."`

**Explanation** The radio's internal temperature exceeds maximum limits on the indicated radio interface.

**Recommended Action** Take steps necessary to reduce the internal temperature. These steps will vary based on your specific installation.

**Error Message** RADIO\_TEMPERATURE\_NORMAL, DOT11, LOG\_INFO, 0, "Interface %s radio temperature returned to normal."

**Explanation** The radio's internal temperature has returned to normal limits on the indicated radio interface.

**Recommended Action** None.

**Error Message** TX\_PWR\_OUT\_OF\_RANGE, DOT11, LOG\_ERR, 0, "Interface %s Radio transmit power out of range."

**Explanation** The transmitter power level is outside the normal range on the indicated radio interface.

**Recommended Action** Remove unit from the network and service.

**Error Message** RADIO\_RF\_LO, DOT11, LOG\_ERR, 0, "Interface %s Radio cannot lock RF freq."

**Explanation** The radio phase lock loop (PLL) circuit is unable to lock the correct frequency on the indicated interface.

**Recommended Action** Remove unit from network and service.

**Error Message** RADIO\_IF\_LO, DOT11, LOG\_ERR, 0, "Interface %s Radio cannot lock IF freq."

**Explanation** The radio intermediate frequency (IF) PLL is unable to lock the correct frequency on the indicated interface.

**Recommended Action** Remove unit from network and service.

**Error Message** FREQ\_SCAN, DOT11, LOG\_INFO, 0, "Interface %s Scanning frequencies for %d seconds."

**Explanation** Starting a scan for a least congested frequency on the interface indicated for a the time period indicated.

**Recommended Action** None.

**Error Message** NO\_CHAN\_AVAIL, DOT11, LOG\_CRIT, 0, "Interface %s, no channel available."

**Explanation** No frequency is available, likely because RADAR has been detected within the previous 30 minutes.

**Recommended Action** None.

**Error Message** DFS\_SCAN\_COMPLETE, DOT11, LOG\_INFO, 0, "DFS scan complete on frequency %d MHz."

**Explanation** The device has completed its Dynamic Frequency Scan (DFS) frequency scanning process on the displayed frequency.

**Recommended Action** None.

**Error Message** DFS\_SCAN\_START, DOT11, LOG\_INFO, 0, "DFS: Scanning frequency %d MHz for %d seconds."

**Explanation** The device has begun its DFS scanning process.

**Recommended Action** None.

**Error Message** DFS\_TRIGGERED, DOT11, LOG\_INFO, 0, "DFS: triggered on frequency %d MHz."

**Explanation** DFS has detected RADAR signals on the indicated frequency.

**Recommended Action** None. The channel will be placed on the non-occupancy list for 30 minutes and a new channel will be selected.

**Error Message** DFS\_STORE\_FAIL, DOT11, LOG\_WARNING, 0, "DFS: could not store the frequency statistics."

**Explanation** A failure occurred writing the DFS statistics to flash.

**Recommended Action** None.

**Error Message** NO\_SSID, DOT11, LOG\_WARNING, 0, "No SSIDs configured, %d not started."

**Explanation** All SSIDs were deleted from the configuration. At least one must be configured for the radio to run.

**Recommended Action** Configure at least one SSID on the access point.

**Error Message** NO\_SSID\_VLAN, DOT11, LOG\_WARNING, 0, "No SSID with VLAN configured. %s not started."

**Explanation** No SSID was configured for a VLAN. The indicated interface was not started.

**Recommended Action** At least one SSID must be configured per VLAN. Add at least one SSID for the VLAN on the indicated interface.

**Error Message** NO\_MBSSID\_VLAN, DOT11, LOG\_WARNING, 0, "No VLANs configured in MBSSID mode. %s not started."

**Explanation** No VLAN configured in MBSSID mode. The indicated interface was not started.

**Recommended Action** Add at least one SSID with the VLAN on the indicated interface configuration.

**Error Message** FW\_LOAD\_DELAYED, DOT11, LOG\_WARNING, 0, "Interface %s, network filesystem not ready. Delaying firmware (%s) load."

**Explanation** The network filesystem was not running or not ready when trying to flash new firmware into the indicated interface. Loading the identified firmware file has been delayed.

**Recommended Action** Make sure the network is up and ready before attempting to reflash the new firmware.

**Error Message** FLASH\_UNKNOWN\_RADIO, DOT11, LOG\_CRIT, 0, "Interface %s has an unknown radio."

**Explanation** The radio type could not be determined when the user attempted to flash new firmware into the indicated interface.

**Recommended Action** Reboot the system and see if the firmware upgrade completes.

**Error Message** UPLINK\_ESTABLISHED, DOT11, LOG\_WARNING, 0, "Interface %s associated to AP %s %e %s."

**Explanation** The indicated repeater has associated to the indicated root access point. Clients can now associate to the indicated repeater and traffic can pass.

**Recommended Action** None.

**Error Message** UPLINK\_FAILED, DOT11, LOG\_CRIT, 0 "Uplink to parent failed: %s."

**Explanation** The connection to the parent access point failed for the displayed reason. The uplink will stop its connection attempts.

**Recommended Action** Try resetting the uplink interface. Contact Technical Support if the problem persists.

**Error Message** CANT\_ASSOC, DOT11, LOG\_WARNING, 0 "Interface %, cannot associate %s."

**Explanation** The indicated interface device could not associate to an indicated parent access point.

**Recommended Action** Check the configuration of the parent access point and this unit to make sure there is a match.

**Error Message** `PROCESS_INITIALIZATION_FAILED, DOT11, LOG_CRIT, 0` "The background process for the radio could not be started: %s)

**Explanation** The initialization process used by the indicated interface failed for some reason, possibly a transient error.

**Recommended Action** Perform a reload of the access point. If this fails to rectify the problem, perform a power cycle. If this still fails, try downgrading the access point firmware to the previous version.

**Error Message** `RADIO_HW_RESET, DOT11, LOG_CRIT, 0` "Radio subsystem is undergoing hardware reset to recover from problem."

**Explanation** An unrecoverable error occurred that could not be resolved by a soft reset.

**Recommended Action** None.

**Error Message** `MAXRETRIES, DOT11, LOG_WARNING, 0`, "Packet to client %e reached max retries, removing the client."

**Explanation** The maximum packet send retry limit has been reached and the client is being removed.

**Recommended Action** Investigate and correct the client malfunction.

**Error Message** `RM_INCAPABLE, DOT11, LOG_WARNING, 0` "Interface %s

**Explanation** Indicated interface does not support the radio management feature.

**Recommended Action** None.

**Error Message** `RM_INCORRECT_INTERFACE, DOT11, LOG_WARNING, 0`, "Invalid interface, either not existing or non-radio."

**Explanation** A radio management request discovered that the interface either does not exist or is not a radio interface.

**Recommended Action** None.

**Error Message** `POWERS_INVALID, DOT11, LOG_ERR, 0`, "Interface %s, no valid power levels available."

**Explanation** The radio driver found no valid power level settings.

**Recommended Action** Investigate and correct the power source and settings.

**Error Message** RADIO\_INVALID\_FREQ, DOT11, LOG\_WARNING, 0, "Operating frequency (%d) invalid - performing a channel scan."

**Explanation** The indicated frequency is invalid for operation. A channel scan is being performed to select a valid frequency.

**Recommended Action** None.

**Error Message** RADIO\_INITIALIZATION\_ERR, DOT11, LOG\_CRIT, 0, "The radio subsystem could not be initialized (%s)."

**Explanation** A critical error was detected while attempting to initialize the radio subsystem.

**Recommended Action** Reload the system.

**Error Message** UPLINK\_NO\_ID\_PWD, DOT11, LOG\_WARNING, 0 "Interface %s, no username/password supplied for uplink authentication."

**Explanation** The user failed to enter a username and/or password.

**Recommended Action** Enter the username and/or password and try again.

**Error Message** NO\_IE\_CFG, DOT11, LOG\_WARNING, MSG\_TRACEBACK, "No IEs configured for %s (ssid index %u)."

**Explanation** When attempting to apply a beacon or probe response to the radio, the beacon or probe was undefined on the indicated SSID index.

**Recommended Action** Check the IE configuration.

**Error Message** FLASHING\_RADIO, DOT11, LOG\_WARNING, 0, "Interface %s, flashing radio firmware (%s)."

**Explanation** The indicated interface radio has been stopped to load the indicated new firmware.

**Recommended Action** None.

**Error Message** LOADING\_RADIO, DOT11, LOG\_WARNING, 0, "Interface %s, loading the radio firmware (%s)."

**Explanation** The indicated interface radio has been stopped to load new indicated firmware.

**Recommended Action** None.



**Error Message** NO\_FIRMWARE, DOT11, LOG\_CRIT, 0 "Interface %s, no radio firmware file (%s) was found."

**Explanation** When trying to flash new firmware, the file for the radio was not found in the Flash file system.

**Recommended Action** The wrong image has been loaded into the unit. Locate the correct image based on the type of radio used.

**Error Message** BAD\_FIRMWARE DOT11, LOG\_CRIT, 0, "Interface %s, radio firmware file (%s) is invalid."

**Explanation** When trying to Flash new firmware into the indicated interface the indicated radio firmware file was found to be invalid.

**Recommended Action** Make sure the correct firmware image file is located in the place where the unit expects to find it.

**Error Message** RADIO\_FAILED, DOT11, LOG\_CRIT, MSG\_TRACEBACK, "Interface %s, failed - %s."

**Explanation** The radio driver on the indicated interface found a severe error and is shutting down for the indicated reason.

**Recommended Action** None.

**Error Message** FLASH\_RADIO\_DONE, DOT11, LOG\_WARNING, 0, "Interface %s, flashing radio firmware completed."

**Explanation** The indicated interface radio firmware flash is complete, and the radio will be restarted with the new firmware.

**Recommended Action** None.

**Error Message** UPLINK\_LINK\_DOWN, DOT11, LOG\_WARNING, 0, "Interface %s, parent lost: %s."

**Explanation** The connection to the parent access point on the indicated interface was lost for the reason indicated. The unit will try to find a new parent access point.

**Recommended Action** None.

**Error Message** CANT\_ASSOC: Cannot associate: [chars]

**Explanation** The unit could not establish a connection to a parent access point for the displayed reason.

**Recommended Action** Verify that the basic configuration settings (SSID, WEP, and others) of the parent access point and this unit match.

**Error Message** DOT11-4-MAXRETRIES: Packet to client [mac] reached max retries, remove the client

**Explanation** A packet sent to the client has not been successfully delivered many times, and the max retries limit has been reached. The client is deleted from the association table.

**Recommended Action** None.

**Error Message** BRIDGE\_LOOP, DOT11, LOG\_WARNING, 0, "Bridge loop detected between WGB %e and device %e."

**Explanation** The indicated workgroup bridge reported the address of one of its indicated Ethernet clients and the access point already had that address marked as being somewhere else on the network.

**Recommended Action** Click **Refresh** on the Associations page on the access point GUI, or enter the **clear dot11 statistics** command on the CLI.

**Error Message** ANTENNA\_INVALID, DOT11, LOG\_WARNING, 0, "Interface %s, current antenna position not supported, radio disabled."

**Explanation** The Indicated AIR-RM21A radio module does not support the high-gain position for the external antenna (the high-gain position is folded flat against the access point). The access point automatically disables the radio when the antenna is in the high-gain position.

**Recommended Action** Fold the antenna on the AIR-RM21A radio module so that it is oriented 90 degrees to the body of the access point.

**Error Message** RF\_LOOPBACK\_FAILURE, DOT11, LOG\_ERR, 0, "Interface %s Radio failed to pass RF loopback test."

**Explanation** Radio loopback test failed for the interface indicated.

**Recommended Action** None.

**Error Message** RF\_LOOPBACK\_\_FREQ\_FAILURE, DOT11, LOG\_ERR, 0, "Interface %s failed to pass RF loopback test."

**Explanation** Radio loopback test failed at a given frequency for the indicated interface.

**Recommended Action** None.

**Error Message** AUTH\_FAILED, DOT11, LOG\_DEBUG, 0, "Station %e Authentication failed," MSDEF\_LIMIT\_MEDIUM

**Explanation** The indicated station failed authentication.

**Recommended Action** Verify that the user entered the correct username and password, and verify that the authentication server is online.

**Error Message** CCKM\_AUTH\_FAILED, DOT11, LOG\_DEBUG, 0, "Station %e CCKM authentication failed."

**Explanation** The indicated station failed CCKM authentication.

**Recommended Action** Verify that the topology of the access points configured to use the WDS access point is functional.

**Error Message** TKIP\_MIC\_FAILURE, DOT11, LOG\_WARNING, 0, "Received TKIP Michael MIC failure report from the station %e on the packet (TSC=0x%11x) encrypted and protected by %s key."

**Explanation** TKIP Michael MIC failure was detected from the indicated station on a unicast frame decrypted locally with the indicated pairwise key.

**Recommended Action** A failure of the Michael MIC in a packet usually indicates an active attack on your network. Search for and remove potential rogue devices from your wireless LAN.

**Error Message** TKIP\_MIC\_FAILURE\_REPORT, DOT11, LOG\_WARNING, 0, "Received TKIP Michael MIC failure report from the station %e on the packet (TSC=0x0) encrypted and protected by %s key"

**Explanation** The access point received an EAPOL-key from the indicated station notifying the access point that TKIP Michael MIC failed on a packet transmitted by this access point.

**Recommended Action** None.

**Error Message** TKIP\_MIC\_FAILURE\_REPEATED, DOT11, LOG\_ERR, 0, "Two TKIP Michael MIC failures were detected within %s seconds on %s interface. The interface will be put on MIC failure hold state for next %d seconds"

**Explanation** Two TKIP Michael MIC failures were detected within the indicated time on the indicated interface. Because this usually indicates an active attack on your network, the interface will be put on hold for the indicated time. During this hold time, stations using TKIP ciphers are disassociated and cannot reassociate until the hold time ends. At the end of the hold time, the interface operates normally.

**Recommended Action** MIC failures usually indicate an active attack on your network. Search for and remove potential rogue devices from your wireless LAN. If this is a false alarm and the interface should not be on hold this long, use the **countermeasure tkip hold-time** command to adjust the hold time.

**Error Message** WGB\_CLIENT\_VLAN\_SOAP, LOG\_ERR, 0: "Workgroup Bridge Ethernet client VLAN not configured."

**Explanation** No VLAN is configured for client devices attached to the workgroup bridge.

**Recommended Action** Configure a VLAN to accommodate client devices attached to the workgroup bridge.

**Error Message** ERROR, SAOP, LOG\_ERR, MSG\_TRACEBACK "Reported on line %d in file %s.%s."

**Explanation** An internal error occurred on the indicated line number in the indicated filename in the controller ASIC.

**Recommended Action** None

## Inter-Access Point Protocol Messages

**Error Message** DSTANDBY\_ACTIVE, DOT11, LOG\_INFO, 0, "Standby to Active, Reason = %s (%d)."

**Explanation** The access point is transitioning from standby mode to active mode for the indicated reason.

**Recommended Action** None.

**Error Message** ROGUE\_AP, DOT11, LOG\_INFO, 0, "Rogue AP %e reported. Reason: %s."

**Explanation** A station has reported a potential rogue access point for the indicated reason.

**Recommended Action** None.

**Error Message** STANDBY\_REQUEST, DOT11, LOG\_INFO, 0, "Hot Standby request to shutdown radios from %e."

**Explanation** The indicated standby access point has requested that this access point shut down its radio interfaces because a failure has been detected on one of this access point's radio interfaces.

**Recommended Action** None.

## Local Authenticator Messages

**Error Message** RADSRV-4-NAS\_UNKNOWN: Unknown authenticator: [ip-address]

**Explanation** The local RADIUS server received an authentication request but does not recognize the IP address of the network access server (NAS) that forwarded the request.

**Recommended Action** Make sure that every access point on your wireless LAN is configured as a NAS on your local RADIUS server.

**Error Message** RADSRV-4-NAS\_KEYMIS: NAS shared key mismatch.

**Explanation** The local RADIUS server received an authentication request but the message signature indicates that the shared key text does not match.

**Recommended Action** Correct the shared key configuration on either the NAS or on the local RADIUS server.

**Error Message** RADSRV-4-BLOCKED: Client blocked due to repeated failed authentications

**Explanation** A user failed authentication the number of times configured to trigger a block, and the account been disabled.

**Recommended Action** Use the **clear radius local-server user *username*** privileged EXEC command to unblock the user, or allow the block on the user to expire by the configured lockout time.

## WDS Messages

**Error Message** WLCCP\_WDS-6-REPEATER\_STOP: WLCCP WDS on Repeater unsupported, WDS is disabled.

**Explanation** Repeater access points do not support WDS.

**Recommended Action** None.

**Error Message** WLCCP\_WDS-6-PREV\_VER\_AP: A previous version of AP is detected.

**Explanation** The WDS device detected a previous version of the access point.

**Recommended Action** None.

**Error Message** WLCCP\_AP-6-INFRA: WLCCP Infrastructure Authenticated

**Explanation** The access point successfully authenticated to the WDS device.

**Recommended Action** None.

**Error Message** WLCCP\_AP-6-STAND\_ALONE: Connection lost to WLCCP server, changing to Stand-Alone Mode

**Explanation** The access point lost its connection to the WDS device and is in stand-alone mode.

**Recommended Action** None.

**Error Message** WLCCP\_AP-6-PREV\_VER\_WDS: A previous version of WDS is detected

**Explanation** The access point detected a previous version of WDS.

**Recommended Action** Check for an unsupported version of WDS on your network.

**Error Message** WLCCP\_AP-6-UNSUP\_VER\_WDS: An unsupported version of WDS is detected

**Explanation** The access point detected an unsupported version of WDS.

**Recommended Action** Check for an unsupported version of WDS on your network.

**Error Message** WLCCP\_NM-3-WNM\_LINK\_DOWN: Link to WNM is down

**Explanation** The network manager is not responding to keep-active messages.

**Recommended Action** Check for a problem with the network manager or with the network path to the network manager.

**Error Message** WLCCP\_NM-6-WNM\_LINK\_UP: Link to WNM is up

**Explanation** The network manager is now responding to keep-active messages.

**Recommended Action** None.

**Error Message** WLCCP\_NM-6-RESET: Resetting WLCCP\_NM

**Explanation** A change in the network manager IP address or a temporary out-of-resource state might have caused a reset on the WDS network manager subsystem, but operation will return to normal shortly.

**Recommended Action** None.

## Mini IOS Messages

**Error Message** PROTECT\_PORT\_FAILURE, MTS, LOG\_CRIT, MSG\_PROCESS: An attempt to protect port [number] failed

**Explanation** Initialization failed on attempting to protect port.

**Recommended Action** None.

**Error Message** SET\_PW\_FAILURE, MTS, LOG\_CRIT, MSG\_PROCESS: Error %d enabling secret password.

**Explanation** Initialization failed when the user attempted to enable a secret password.

**Recommended Action** None



## GLOSSARY

- 802.11** The IEEE standard that specifies carrier sense media access control and physical layer specifications for 1- and 2-megabit-per-second (Mbps) wireless LANs operating in the 2.4-GHz band.
- 802.11b** The IEEE standard that specifies carrier sense media access control and physical layer specifications for 5.5- and 11-Mbps wireless LANs operating in the 2.4-GHz frequency band.
- 802.11g** The IEEE standard that specifies carrier sense media access control and physical layer specifications for wireless LANs operating in the 2.4-GHz frequency band.
- 802.11af** The IEEE standard that specifies a mechanism for Power over Ethernet (PoE). The standard provides the capability to deliver both power and data over standard Ethernet cabling.

---

## A

- access point** A wireless LAN data transceiver that uses radio waves to connect a wired network with wireless stations.
- ad hoc network** A wireless network composed of stations without access points.
- antenna gain** The gain of an antenna is a measure of the antenna's ability to direct or focus radio energy over a region of space. High-gain antennas have a more focused radiation pattern in a specific direction.
- associated** A station is configured properly to enable it to wirelessly communicate with an access point.

---

## B

- beacon** A wireless LAN packet that signals the availability and presence of the wireless device.
- BID** Bridge identifier used in spanning-tree calculations. The BID contains the bridge MAC address and its spanning-tree priority value. If all bridges in the spanning tree are assigned the same priority, the bridge with the lowest MAC address becomes the spanning-tree root.
- BOOTP** Boot Protocol. A protocol used for the static assignment of IP addresses to devices on the network.

|                         |                                                                                                                                                                                       |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>BPDU</b>             | Bridge protocol data unit. When STP is enabled, bridges send and receive spanning-tree frames, called BPDUs, at regular intervals and use the frames to maintain a loop-free network. |
| <b>BPSK</b>             | A modulation technique used by IEEE 802.11b-compliant wireless LANs for transmission at 1 Mbps.                                                                                       |
| <b>broadcast packet</b> | A single data message (packet) sent to all addresses on the same subnet.                                                                                                              |

---

## C

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CCK</b>    | Complementary code keying. A modulation technique used by IEEE 802.11b-compliant wireless LANs for transmission at 5.5 and 11 Mbps.                                                                                                                                                                                                                                                                                                                                                               |
| <b>CCKM</b>   | Cisco Centralized Key Management. Using CCKM, authenticated client devices can roam from one access point to another without any perceptible delay during reassociation. An access point on your network acts as a subnet context manager (SCM) and creates a cache of security credentials for CCKM-enabled client devices on the subnet. The SCM's cache of credentials dramatically reduces the time required for reassociation when a CCKM-enabled client device roams to a new access point. |
| <b>cell</b>   | The area of radio range or coverage in which the wireless devices can communicate with the base station. The size of the cell depends upon the speed of the transmission, the type of antenna used, and the physical environment, as well as other factors.                                                                                                                                                                                                                                       |
| <b>client</b> | A radio device that uses the services of an access point to communicate wirelessly with other devices on a local area network.                                                                                                                                                                                                                                                                                                                                                                    |
| <b>CSMA</b>   | Carrier sense multiple access. A wireless LAN media access method specified by the IEEE 802.11 specification.                                                                                                                                                                                                                                                                                                                                                                                     |

---

## D

|                   |                                                                                                                                                                                                                                                                       |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>data rates</b> | The range of data transmission rates supported by a device. Data rates are measured in megabits per second (Mbps).                                                                                                                                                    |
| <b>dBi</b>        | A ratio of decibels to an isotropic antenna that is commonly used to measure antenna gain. The greater the dBi value, the higher the gain, and the more acute the angle of coverage.                                                                                  |
| <b>DHCP</b>       | Dynamic host configuration protocol. A protocol available with many operating systems that automatically issues IP addresses within a specified range to devices on the network. The device retains the assigned address for a specific administrator-defined period. |
| <b>dipole</b>     | A type of low-gain (2.2-dBi) antenna consisting of two (often internal) elements.                                                                                                                                                                                     |



|                    |                                                                                                                                                                                                                                                                                                |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>domain name</b> | The text name that refers to a grouping of networks or network resources based on organization-type or geography; for example: name.com—commercial; name.edu—educational; name.gov—government; ISPname.net—network provider (such as an ISP); name.ar—Argentina; name.au—Australia; and so on. |
| <b>DNS</b>         | Domain Name System server. A server that translates text names into IP addresses. The server maintains a database of host alphanumeric names and their corresponding IP addresses.                                                                                                             |
| <b>DSSS</b>        | Direct sequence spread spectrum. A type of spread spectrum radio transmission that spreads its signal continuously over a wide frequency band.                                                                                                                                                 |

---

## E

|                 |                                                                                                                                                                                                                      |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>EAP</b>      | Extensible Authentication Protocol. An optional IEEE 802.1x security feature ideal for organizations with a large user base and access to an EAP-enabled Remote Authentication Dial-In User Service (RADIUS) server. |
| <b>Ethernet</b> | The most widely used wired local area network. Ethernet uses carrier sense multiple access (CSMA) to allow computers to share a network and operates at 10, 100, or 1000 Mbps, depending on the physical layer used. |

---

## F

|                    |                                                                                          |
|--------------------|------------------------------------------------------------------------------------------|
| <b>file server</b> | A repository for files so that a local area network can share files, mail, and programs. |
| <b>firmware</b>    | Software that is programmed on a memory chip.                                            |

---

## G

|                |                                                                            |
|----------------|----------------------------------------------------------------------------|
| <b>gateway</b> | A device that connects two otherwise incompatible networks.                |
| <b>GHz</b>     | Gigahertz. One billion cycles per second. A unit of measure for frequency. |

---

## I

|                       |                                                                                                                                                                                                                                                                        |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>IEEE</b>           | Institute of Electrical and Electronic Engineers. A professional society serving electrical engineers through its publications, conferences, and standards development activities. The body responsible for the Ethernet 802.3 and wireless LAN 802.11 specifications. |
| <b>infrastructure</b> | The wired Ethernet network.                                                                                                                                                                                                                                            |
| <b>IP address</b>     | The Internet Protocol (IP) address of a station.                                                                                                                                                                                                                       |

**IP subnet mask** The number used to identify the IP subnetwork, indicating whether the IP address can be recognized on the LAN or if it must be reached through a gateway. This number is expressed in a form similar to an IP address; for example: 255.255.255.0.

**isotropic** An antenna that radiates its signal in a spherical pattern.

---

## M

**MAC** Media Access Control address. A unique 48-bit number used in Ethernet data packets to identify an Ethernet device such as an access point or your client adapter.

**modulation** Any of several techniques for combining user information with a transmitter's carrier signal.

**multipath** The echoes created as a radio signal bounces off of physical objects.

**multicast packet** A single data message (packet) sent to multiple addresses.

---

## O

**omni-directional** This typically refers to a primarily circular antenna radiation pattern.

**Orthogonal Frequency Division Multiplex (OFDM)** A modulation technique used by IEEE 802.11a-compliant wireless LANs for transmission at 6, 9, 12, 18, 24, 36, 48, and 54 Mbps.

---

## P

**packet** A basic message unit for communication across a network. A packet usually includes routing information, data, and sometimes error detection information.

---

## Q

**quadruple phase shift keying** A modulation technique used by IEEE 802.11b-compliant wireless LANs for transmission at 2 Mbps.

---

## R

**range** A linear measure of the distance that a transmitter can send a signal.

**receiver sensitivity** A measurement of the weakest signal a receiver can receive and still correctly translate it into data.

|                |                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>RF</b>      | Radio frequency. A generic term for radio-based technology.                                                                                                                                                                                                                                                                                                                                                 |
| <b>roaming</b> | A feature of some access points that allows users to move through a facility while maintaining an unbroken connection to the LAN.                                                                                                                                                                                                                                                                           |
| <b>RP-TNC</b>  | A connector type unique to Cisco Aironet radios and antennas. Part 15.203 of the FCC rules covering spread spectrum devices limits the types of antennas that may be used with transmission equipment. In compliance with this rule, Cisco Aironet, like all other wireless LAN providers, equips its radios and antennas with a unique connector to prevent attachment of non-approved antennas to radios. |

---

## S

|                        |                                                                                                                                                                                                                                                                                             |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>spread spectrum</b> | A radio transmission technology that spreads the user information over a much wider bandwidth than otherwise required in order to gain benefits such as improved interference tolerance and unlicensed operation.                                                                           |
| <b>SSID</b>            | Service Set Identifier (also referred to as Radio Network Name). A unique identifier used to identify a radio network and which stations must use to be able to communicate with each other or to an access point. The SSID can be any alphanumeric entry up to a maximum of 32 characters. |

---

## T

|                       |                                        |
|-----------------------|----------------------------------------|
| <b>transmit power</b> | The power level of radio transmission. |
|-----------------------|----------------------------------------|

---

## U

|                       |                                                                                                                                                         |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>UNII</b>           | Unlicensed National Information Infrastructure—regulations for UNII devices operating in the 5.15- to 5.35-GHz and 5.725- to 5.825-GHz frequency bands. |
| <b>UNII-1</b>         | Regulations for UNII devices operating in the 5.15- to 5.25-GHz frequency band.                                                                         |
| <b>UNII-2</b>         | Regulations for UNII devices operating in the 5.25- to 5.35-GHz frequency band.                                                                         |
| <b>UNII-3</b>         | Regulations for UNII devices operating in the 5.725- to 5.825-GHz frequency band.                                                                       |
| <b>unicast packet</b> | A single data message (packet) sent to a specific IP address.                                                                                           |

---

**W**

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>WDS</b>         | Wireless Domain Services. An access point providing WDS on your wireless LAN maintains a cache of credentials for CCKM-capable client devices on your wireless LAN. When a CCKM-capable client roams from one access point to another, the WDS access point forwards the client's credentials to the new access point with the multicast key. Only two packets pass between the client and the new access point, greatly shortening the reassociation time.                                                           |
| <b>WEP</b>         | Wired Equivalent Privacy. An optional security mechanism defined within the 802.11 standard designed to make the link integrity of wireless devices equal to that of a cable.                                                                                                                                                                                                                                                                                                                                         |
| <b>WLSE</b>        | Wireless LAN Solutions Engine. The WLSE is a specialized appliance for managing Cisco Aironet wireless LAN infrastructures. It centrally identifies and configures access points in customer-defined groups and reports on throughput and client associations. WLSE centralized management capabilities are further enhanced with an integrated template-based configuration tool for added configuration ease and improved productivity.                                                                             |
| <b>workstation</b> | A computing device with an installed client adapter.                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>WPA</b>         | Wi-Fi Protected Access (WPA) is the new interim security solution from the Wireless Ethernet Compatibility Alliance (WECA). WPA, mostly synonymous to Simple Security Network (SSN), relies on the interim version of IEEE Standard 802.11i. WPA supports WEP and TKIP encryption algorithms as well as 802.1X and EAP for simple integration with existing authentication systems. WPA key management uses a combination of encryption methods to protect communication between client devices and the access point. |



---

## Numerics

350 series bridge interoperability [8-3](#)

802.11g [6-19](#)

---

## A

abbreviating commands [4-3](#)

access point security settings, matching client devices [10-15](#)

accounting

with RADIUS [12-12](#)

with TACACS+ [12-21, 12-26](#)

accounting command [7-5](#)

AES-CCMP [9-2](#)

Aironet Client Utility (ACU) [21-6](#)

antenna gains

setting [6-14](#)

Apply button [3-4](#)

ARP

caching [5-24](#)

associations, limiting by MAC address [15-5](#)

attributes, RADIUS

sent by the access point [12-18](#)

vendor-proprietary [12-15](#)

vendor-specific [12-14](#)

authentication

local mode with AAA [5-17](#)

NTP associations [5-28](#)

RADIUS

key [12-5](#)

login [5-9, 12-7](#)

SSID [7-2](#)

TACACS+

defined [12-21](#)

key [12-23](#)

login [5-14, 12-24](#)

authentication client command [7-4](#)

authentication server

EAP [10-4, 12-3](#)

authentication types

Network-EAP [10-4](#)

open [10-2](#)

shared key [10-3](#)

authoritative time source, described [5-26](#)

authorization

with RADIUS [5-12, 12-11](#)

with TACACS+ [5-15, 12-21, 12-25](#)

AVVID priority mapping [14-11](#)

---

## B

Back button [3-4](#)

backoff [6-19](#)

bandwidth [6-9](#)

banners

configuring

login [5-42](#)

message-of-the-day login [5-41](#)

default configuration [5-41](#)

when displayed [5-41](#)

basic settings, checking [21-5](#)

beacon dtim-period command [6-19](#)

blocking communication between clients [6-17](#)

BR350 interoperability [8-3](#)

broadcast key rotation [9-1, 9-3](#)

BSSIDs [7-7](#)

## C

Called-Station-ID

See CSID

Cancel button [3-4](#)

capture frames [11-27](#)

carrier busy test [6-22](#)

Catalyst 6500 Series [11-1](#)

CCKM [10-6](#)

authenticated clients [10-6](#)

CCK modulation [6-8](#)

CDP

disabling for routing device [16-4](#)

enabling and disabling

on an interface [16-4](#)

monitoring [16-5](#)

Cisco TAC [21-1](#)

CiscoWorks 2000 [17-4](#)

CLI

abbreviating commands [4-3](#)

command modes [4-2](#)

editing features

enabling and disabling [4-6](#)

keystroke editing [4-6](#)

wrapped lines [4-7](#)

error messages [4-4](#)

filtering command output [4-8](#)

getting help [4-3](#)

history

changing the buffer size [4-4](#)

described [4-4](#)

disabling [4-5](#)

recalling commands [4-5](#)

no and default forms of commands [4-3](#)

using Telnet to access [2-19](#)

client ARP caching [5-24](#)

client communication, blocking [6-17](#)

clock

See system clock

command-line interface

See CLI

command modes [4-2](#)

commands

abbreviating [4-3](#)

accounting [7-5](#)

authentication client [7-4](#)

beacon dtim-period [6-19](#)

encryption [9-4](#)

guest-mode [7-5](#)

infrastructure-ssid [7-5](#)

ip redirect [7-12](#)

no and default [4-3](#)

permit tcp-port [7-12](#)

power client [6-9](#)

setting privilege levels [5-7](#)

show dot11 associations [7-6](#)

slot-time-short [6-19](#)

ssid [7-4](#)

vlan [7-5](#)

community strings

configuring [17-5](#)

overview [17-4](#)

configuration files

creating using a text editor [18-10](#)

deleting a stored configuration [18-18](#)

downloading

preparing [18-10, 18-13, 18-16](#)

reasons for [18-8](#)

using FTP [18-13](#)

using RCP [18-17](#)

using TFTP [18-11](#)

guidelines for creating and using [18-9](#)

invalid combinations when copying [18-5](#)

system contact and location information [17-10](#)

types and location [18-10](#)

uploading

preparing [18-10, 18-13, 18-16](#)

reasons for [18-8](#)

- using FTP [18-14](#)
- using RCP [18-18](#)
- using TFTP [18-12](#)
- connections, secure remote [5-24](#)
- crypto software image [5-23](#)
- CSID format, selecting [12-13](#)

## D

- Data Beacon Rate [6-19](#)
- daylight saving time [5-37](#)
- default commands [4-3](#)
- default configuration
  - banners [5-41](#)
  - DNS [5-40](#)
  - NTP [5-28](#)
  - password and privilege level [5-3](#)
  - RADIUS [5-8, 12-4](#)
  - resetting [2-19, 21-6](#)
  - SNMP [17-5](#)
  - system message logging [19-3](#)
  - system name and prompt [5-39](#)
  - TACACS+ [5-14, 12-23](#)
- delivery traffic indication message (DTIM) [6-19](#)
- DHCP server
  - configuring access point as [5-21](#)
- directories
  - changing [18-4](#)
  - creating and removing [18-4](#)
  - displaying the working [18-4](#)
- disable web-based management [3-14](#)
- distance setting [6-16](#)
- DNS
  - default configuration [5-40](#)
  - displaying the configuration [5-41](#)
  - overview [5-39](#)
  - setting up [5-40](#)
- domain names
  - DNS [5-39](#)

## Domain Name System

- See DNS

## downloading

- configuration files
  - preparing [18-10, 18-13, 18-16](#)
  - reasons for [18-8](#)
  - using FTP [18-13](#)
  - using RCP [18-17](#)
  - using TFTP [18-11](#)
- image files
  - deleting old image [18-22](#)
  - preparing [18-20, 18-24, 18-28](#)
  - reasons for [18-19](#)
  - using FTP [18-25](#)
  - using RCP [18-30](#)
  - using TFTP [18-21](#)

## DTIM [6-19](#)

## E

- EAP authentication
  - overview [10-4](#)
- EAP-TLS authentication
  - setting on client and access point [10-16](#)
- editing features
  - enabling and disabling [4-6](#)
  - keystrokes used [4-6](#)
  - wrapped lines [4-7](#)
- enable password [5-4](#)
- enable secret password [5-4](#)
- encrypted software image [5-23](#)
- encryption command [9-4](#)
- encryption for passwords [5-4](#)
- error and event messages [D-1](#)
- error messages
  - 802.11 subsystem messages [D-5](#)
  - association management messages [D-3](#)
  - during command entry [4-4](#)
  - explained [D-1](#)

- inter-access point protocol messages [D-14](#)
- local authenticator messages [D-14](#)
- setting the display destination device [19-5](#)
- severity levels [19-7](#)
- software auto upgrade messages [D-2](#)
- system message format [19-2](#)
- unzip messages [D-4](#)

Ethernet and duplex settings

- configuring [5-16](#)

event messages [D-1](#)

Express Security page [2-10](#)

## F

fast secure roaming [11-1](#)

files

- copying [18-5](#)
- deleting [18-5](#)
- displaying the contents of [18-8](#)
- tar
  - creating [18-6](#)
  - displaying the contents of [18-7](#)
  - extracting [18-7](#)
  - image file format [18-20](#)

file system

- displaying available file systems [18-2](#)
- displaying file information [18-3](#)
- local file system names [18-2](#)
- network file system names [18-5](#)
- setting the default [18-3](#)

filtering

- show and more command output [4-8](#)

Flash device, number of [18-2](#)

forward-delay time

- STP [8-7](#)

fragmentation threshold [6-21](#)

frequencies [6-10](#)

FTP

- accessing MIB files [C-2](#)

configuration files

- downloading [18-13](#)
- overview [18-12](#)
- preparing the server [18-13](#)
- uploading [18-14](#)

image files

- deleting old image [18-27](#)
- downloading [18-25](#)
- preparing the server [18-24](#)
- uploading [18-27](#)

## G

get-bulk-request operation [17-3](#)

get-next-request operation [17-3, 17-4](#)

get-request operation [17-3, 17-4](#)

get-response operation [17-3](#)

global configuration mode [4-2](#)

group key updates [10-13](#)

guest mode [7-2](#)

guest-mode command [7-5](#)

guest SSID [7-2](#)

## H

help, for the command line [4-3](#)

history

- changing the buffer size [4-4](#)
- described [4-4](#)
- disabling [4-5](#)
- recalling commands [4-5](#)

history table, level and number of syslog messages [19-8](#)

Home button [3-3](#)

hot standby

- configuring [20-7](#)
- verifying operation [20-10](#)

HTTPS [3-4](#)



**I**

IGMP snooping helper [14-11](#)  
 infrastructure device [7-5](#)  
 infrastructure-ssid command [7-5](#)  
 inter-client communication, blocking [6-17](#)  
 interface configuration mode [4-2](#)  
 intrusion detection [11-1](#)  
 IP address, finding and setting [2-18](#)  
 ip redirect command [7-12](#)  
 IP redirection [7-10, 7-11](#)  
 IPSU [2-17](#)  
 ISO designators for protocols [B-1](#)

**K**

key features [1-2](#)

**L**

Layer 3 mobility [11-4](#)  
 LEAP  
     described [1-2](#)  
 LEAP authentication  
     setting on client and access point [10-16](#)  
 Light Extensible Authentication Protocol  
     See LEAP  
 limiting client associations by MAC address [15-5](#)  
 login authentication  
     with RADIUS [5-9, 12-7](#)  
     with TACACS+ [5-14, 12-24](#)  
 login banners [5-41](#)  
 log messages  
     See system message logging

**M**

MAC [2-18](#)  
 MAC address

ACLs, blocking association with [15-5](#)  
     troubleshooting [21-6](#)  
 management options  
     CLI [4-1](#)  
 Message Integrity Check (MIC) [1-2, 9-1, 21-6](#)  
 messages  
     to users through banners [5-41](#)  
 MIBs  
     accessing files with FTP [C-2](#)  
     location of files [C-2](#)  
     overview [17-2](#)  
     SNMP interaction with [17-4](#)  
 MIC [9-1](#)  
 Microsoft IAS servers [10-2](#)  
 migration mode, WPA [10-12](#)  
 mobile station command [6-4](#)  
 monitoring  
     CDP [16-5](#)  
 monitor mode [11-27](#)  
 multiple basic SSIDs [7-7](#)

**N**

names, VLAN [13-7](#)  
 Network-EAP [10-4](#)  
 Network Time Protocol  
     See NTP  
 no commands [4-3](#)  
 NTP  
     associations  
         authenticating [5-28](#)  
         defined [5-27](#)  
         enabling broadcast messages [5-31](#)  
         peer [5-30](#)  
         server [5-30](#)  
     default configuration [5-28](#)  
     displaying the configuration [5-35](#)  
     overview [5-26](#)  
     restricting access

- creating an access group [5-33](#)
- disabling NTP services per interface [5-34](#)
- source IP address, configuring [5-34](#)
- stratum [5-26](#)
- synchronizing devices [5-30](#)
- time
  - services [5-27](#)
  - synchronizing [5-26](#)

## O

- OFDM modulation [6-8](#)
- OK button [3-4](#)
- optional ARP caching [5-25](#)

## P

- passwords
  - default configuration [5-3](#)
  - encrypting [5-4](#)
  - overview [5-2](#)
  - setting
    - enable [5-3](#)
    - enable secret [5-4](#)
    - with usernames [5-6](#)
- PEAP authentication
  - setting on client and access point [10-17](#)
- permit tcp-port command [7-12](#)
- per-VLAN Spanning Tree (PVST) [8-2](#)
- ports, protected [6-18](#)
- power client command [6-9](#)
- power-save client device [6-19](#)
- preferential treatment of traffic
  - See QoS
- pre-shared key [10-13](#)
- preventing unauthorized access [5-2](#)
- privileged EXEC mode [4-2](#)
- privilege levels
  - exiting [5-8](#)

- logging into [5-8](#)
- overview [5-2, 5-6](#)
- setting a command with [5-7](#)
- Public Secure Packet Forwarding [6-17](#)

## Q

- QBSS [14-3](#)
  - dot11e parameter [14-3](#)
- QoS
  - configuration guidelines [14-5](#)
  - described [1-2](#)
  - overview [14-2](#)
- quality of service
  - See QoS

## R

- radio
  - congestion [6-9](#)
  - distance setting [6-16](#)
  - enabling [6-2](#)
  - role in radio network [6-2](#)
- radio management [11-1](#)
- RADIUS
  - attributes
    - CSID format, selecting [12-13](#)
    - sent by the access point [12-18](#)
    - vendor-proprietary [12-15](#)
    - vendor-specific [12-14](#)
    - WISPr [12-16](#)
  - configuring
    - accounting [12-12](#)
    - authentication [5-9, 12-7](#)
    - authorization [5-12, 12-11](#)
    - communication, global [12-5, 12-13](#)
    - communication, per-server [12-5](#)
    - multiple UDP ports [12-5](#)
    - default configuration [5-8, 12-4](#)

- defining AAA server groups [5-10, 12-9](#)
- displaying the configuration [5-13, 12-17](#)
- identifying the server [12-5](#)
- limiting the services to the user [5-12, 12-11](#)
- method list, defined [12-4](#)
- operation of [12-3](#)
- overview [12-2](#)
- SSID [7-2](#)
- suggested network environments [12-2](#)
- tracking services accessed by user [12-12](#)
- rate limit, logging [19-9](#)

## RCP

- configuration files
  - downloading [18-17](#)
  - overview [18-15](#)
  - preparing the server [18-16](#)
  - uploading [18-18](#)
- image files
  - deleting old image [18-31](#)
  - downloading [18-30](#)
  - preparing the server [18-28](#)
  - uploading [18-32](#)
- reauthentication requests [10-2](#)
- redirection, IP [7-10](#)
- regulatory
  - domains [6-10](#)
- reloading bridge image [21-9](#)
- Remote Authentication Dial-In User Service
  - See RADIUS
- Remote Copy Protocol
  - See RCP
- repeater
  - as a LEAP client [20-5](#)
  - as a WPA client [20-6](#)
  - chain of access points [20-2](#)
- restricting access
  - NTP services [5-32](#)
  - overview [5-2](#)
  - passwords and privilege levels [5-2](#)

- RADIUS [5-8, 12-1](#)
- TACACS+ [5-13](#)
- RFC
  - 1157, SNMPv1 [17-2](#)
  - 1305, NTP [5-26](#)
  - 1901, SNMPv2C [17-2](#)
  - 1902 to 1907, SNMPv2 [17-2](#)
- roaming
  - fast secure roaming using CCKM [11-1](#)
- rotation, broadcast key [9-1](#)
- RTS threshold [6-19](#)

## S

- secure remote connections [5-24](#)
- Secure Shell
  - See SSH
- security
  - troubleshooting [21-6](#)
- security features [1-2](#)
  - synchronizing [10-15](#)
- security settings, Express Security page [2-10](#)
- self-healing wireless LAN [11-4](#)
- sequence numbers in log messages [19-6](#)
- serial
  - serial port connector [2-3, 4-9, 21-4](#)
- service set identifiers (SSIDs)
  - See SSID
- service-type attribute [10-2](#)
- set-request operation [17-4](#)
- severity levels, defining in system messages [19-7](#)
- shared key [10-6](#)
- short slot time [6-19](#)
- show cdp traffic command [16-5](#)
- show dot11 associations command [7-6](#)
- Simple Network Management Protocol
  - See SNMP
- slot time, short [6-19](#)
- slot-time-short command [6-19](#)

## SNMP

- accessing MIB variables with [17-4](#)
  - agent
    - described [17-3](#)
    - disabling [17-5](#)
  - community strings
    - configuring [17-5](#)
    - overview [17-4](#)
  - configuration examples [17-10](#)
  - default configuration [17-5](#)
  - limiting system log messages to NMS [19-8](#)
  - manager functions [17-3](#)
  - overview [17-2, 17-4](#)
  - snmp-server view [17-10](#)
  - status, displaying [17-11](#)
  - system contact and location [17-10](#)
  - trap manager, configuring [17-9](#)
  - traps
    - described [17-3](#)
    - enabling [17-7](#)
    - overview [17-2, 17-4](#)
    - types of [17-7](#)
  - versions supported [17-2](#)
- SNMP, FTP MIB files [C-2](#)
- snooping helper, IGMP [14-11](#)
- software images
  - location in Flash [18-19](#)
  - tar file format, described [18-20](#)
- software upgrade
  - error and event messages [D-2](#)
- spaces in an SSID [7-6](#)
- SSH [4-9](#)
  - configuring [5-24](#)
  - crypto software image [5-23](#)
  - described [5-24](#)
  - displaying settings [5-24](#)
  - SSH Communications Security, Ltd. [4-9](#)
- SSID [7-2](#)
  - guest mode [7-2](#)

multiple SSIDs [7-1](#)

support [1-2](#)

troubleshooting [21-5](#)

using spaces in [7-6](#)

VLAN [7-2](#)

SSID, troubleshooting [21-5](#)

ssid command [7-4](#)

SSL [3-4](#)

static WEP

- with open authentication, setting on client and access point [10-15](#)

- with shared key authentication, setting on client and access point [10-15](#)

statistics

- CDP [16-5](#)

- SNMP input and output [17-11](#)

STP

- BPDU message exchange [8-3](#)

- designated port, defined [8-4](#)

- designated switch, defined [8-4](#)

- displaying status [8-14](#)

- inferior BPDU [8-4](#)

interface states

- blocking [8-7](#)

- disabled [8-8](#)

- forwarding [8-7, 8-8](#)

- learning [8-8](#)

- listening [8-7](#)

- overview [8-6](#)

overview [8-2](#)

- root port, defined [8-4](#)

- superior BPDU [8-4](#)

- timers, described [8-5](#)

stratum, NTP [5-26](#)

summer time [5-37](#)

switchport protected command [6-18](#)

syslog

- See system message logging

system clock

- configuring
    - daylight saving time [5-37](#)
    - manually [5-35](#)
    - summer time [5-37](#)
    - time zones [5-36](#)
  - displaying the time and date [5-36](#)
  - overview [5-26](#)
  - See also NTP
  - system message logging
    - default configuration [19-3](#)
    - defining error message severity levels [19-7](#)
    - disabling [19-4](#)
    - displaying the configuration [19-12](#)
    - enabling [19-4](#)
    - facility keywords, described [19-11](#)
    - level keywords, described [19-8](#)
    - limiting messages [19-8](#)
    - message format [19-2](#)
    - overview [19-2](#)
    - rate limit [19-9](#)
    - sequence numbers, enabling and disabling [19-6](#)
    - setting the display destination device [19-5](#)
    - timestamps, enabling and disabling [19-6](#)
  - UNIX syslog servers
    - configuring the daemon [19-10](#)
    - configuring the logging facility [19-10](#)
    - facilities supported [19-11](#)
  - system name
    - default configuration [5-39](#)
    - manual configuration [5-39](#)
  - See also DNS
  - system prompt
    - default setting [5-38](#), [5-39](#)
  - authentication, defined [12-21](#)
  - authorization, defined [12-21](#)
  - configuring
    - accounting [12-26](#)
    - authentication key [12-23](#)
    - authorization [5-15](#), [12-25](#)
    - login authentication [5-14](#), [12-24](#)
  - default configuration [5-14](#), [12-23](#)
  - described [1-2](#)
  - displaying the configuration [5-16](#), [12-27](#)
  - identifying the server [12-23](#)
  - limiting the services to the user [5-15](#), [12-25](#)
  - operation of [12-22](#)
  - overview [12-21](#)
  - tracking services accessed by user [12-26](#)
  - tar files
    - creating [18-6](#)
    - displaying the contents of [18-7](#)
    - extracting [18-7](#)
    - image file format [18-20](#)
  - Telnet [2-19](#)
  - Temporal Key Integrity Protocol (TKIP) [9-1](#)
  - Terminal Access Controller Access Control System Plus
    - See TACACS+
  - TFTP
    - configuration files
      - downloading [18-11](#)
      - preparing the server [18-10](#)
      - uploading [18-12](#)
    - image files
      - deleting [18-22](#)
      - downloading [18-21](#)
      - preparing the server [18-20](#)
      - uploading [18-23](#)
  - time
    - See NTP and system clock
  - timestamps in log messages [19-6](#)
  - time zones [5-36](#)
  - TKIP [9-1](#), [9-2](#)
- ## T
- TAC [21-1](#)
  - TACACS+
    - accounting, defined [12-21](#)

## traps

- configuring managers [17-7](#)
- defined [17-3](#)
- enabling [17-7](#)
- notification types [17-7](#)
- overview [17-2, 17-4](#)

troubleshooting [21-1](#)

- with CiscoWorks [17-4](#)
- with system message logging [19-2](#)

**U**

## UNIX syslog servers

- daemon configuration [19-10](#)
- facilities supported [19-11](#)
- message logging configuration [19-10](#)

## upgrading software images

- See downloading

## uploading

- configuration files
  - preparing [18-10, 18-13, 18-16](#)
  - reasons for [18-8](#)
  - using FTP [18-14](#)
  - using RCP [18-18](#)
  - using TFTP [18-12](#)

## image files

- preparing [18-20, 18-24, 18-28](#)
- reasons for [18-19](#)
- using FTP [18-27](#)
- using RCP [18-32](#)
- using TFTP [18-23](#)

user EXEC mode [4-2](#)username-based authentication [5-6](#)**V**

## VLAN

- configuration example [13-9](#)
- configuring [13-4](#)

creating a VLAN name [13-8](#)

guidelines for names [13-7](#)

incorporating access points into [13-4](#)

names [13-7](#)

SSID [7-2](#)

using RADIUS server to assign users [13-8](#)

viewing on access point/bridge [13-7](#)

vlan command [7-5](#)

**W**

WDS [11-1, 11-8](#)

## Web-based interface

- common buttons [3-3](#)

## web site

- Cisco Software Center [2-17](#)

## WEP

- key example [9-5](#)
- key hashing [1-2](#)
- with EAP [10-4](#)

WEP key [21-6](#)

- troubleshooting [21-6](#)

WIDS [11-6](#)Wi-Fi Multimedia [14-4](#)

## Wi-Fi Protected Access

- See WPA

wireless intrusion detection services [11-1](#)Wireless LAN Services Module [11-2](#)WISPr RADIUS attributes [12-16](#)WMM [14-4](#)

## workgroup bridge

- configuring [20-13](#)
- configuring client VLAN [20-13](#)
- configuring for roaming [20-13](#)
- treating as infrastructure or client devices [20-12](#)
- understanding [20-11](#)

world mode [1-2](#)

## world-mode

- 802.11d standard [6-11](#)

Cisco legacy [6-11](#)  
WPA [10-7](#)  
WPA migration mode [10-12](#)

