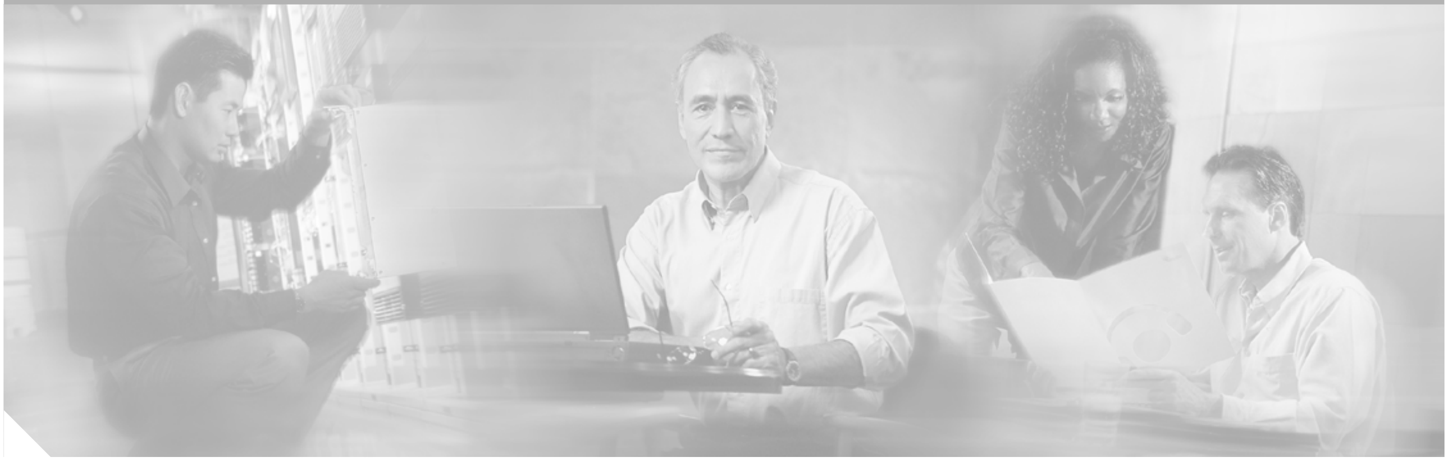


Cisco 3200 Series Wireless MIC Software Configuration Guide

June 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-7734-02

CONTENTS

CHAPTER 16

CHAPTER 17

APPENDIX A

Preface

Audience

This guide is for the networking professional who installs and manages Cisco 3200 Series Mobile Access Routers. 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 bridge. This guide provides procedures for using the IOS commands that have been created or changed for use with the WMIC. It does not provide detailed information about these commands. For detailed information about these commands, refer to the IOS documentation set available from the Cisco.com home page at **Service and Support > Technical Documents**. On the Cisco Product Documentation home page, select **Release 12.3** from the Cisco IOS Software drop-down list.

This guide includes an overview of the web-based interface, which contains all the funtionality 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 WMIC from the web-based interface. For all window descriptions and procedures, refer to the 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 WMIC and describes the WMIC's role in your network.

Chapter 2, "Configuring the WMIC for the First Time," describes how to configure basic settings on a Wireless Mobile Interface Card (WMIC) for the first time.

Chapter 3, "Administering the WMIC," describes how to perform one-time operations to administer your WMIC, such as preventing unauthorized access to the device, setting the system date and time, and setting the system name and prompt.

Chapter 4, "Configuring Radio Settings," describes how to configure settings for the WMIC radio such as the role in the radio network, data rates, transmit power, channel settings, and others.

Chapter 5, "Configuring SSIDs," describes how to configure and manage multiple service set identifiers (SSIDs). You can configure up to 16 SSIDs and assign different configuration settings to each SSID.

Chapter 6, "Configuring Spanning Tree Protocol," descibes how to configure Spanning Tree Protocol (STP). STP prevents data loops in your network.

Chapter 7, "Configuring WEP and WEP Features," 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 8, "Configuring Authentication Types," describes how to configure authentication types. Client devices use these authentication methods to join your network.

Chapter 9, "Configuring WDS, Fast Secure Roaming, and Radio Management," describes Wireless Domain Services (WDS), fast secure roaming, and radio management features. The chapter also provides instructions for configuring the WMIC to register with a WDS access point.

Chapter 10, "Configuring VLANs," describes how to configure your WMIC to interoperate with the VLANs set up on your wired LAN.

Chapter 11, "Configuring QoS in a Wireless Environment," describes how to configure quality of service (QoS) on your WMIC. With this feature, you can provide preferential treatment to certain traffic at the expense of others.

Chapter 12, "Configuring Filters," describes how to configure and manage MAC address, IP, and Ethertype filters on the WMICWMIC by using the web-browser interface.

Chapter 13, "Configuring CDP," describes how to configure Cisco Discovery Protocol (CDP) on your WMIC. CDP is a device-discovery protocol that runs on all Cisco network equipment.

Chapter 14, "Configuring SNMP," describes how to configure the Simple Network Management Protocol (SNMP) on your WMIC.

Chapter 15, "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 16, "Configuring System Message Logging," describes how to configure system message logging on your WMIC.

Chapter 17, "Wireless Device Troubleshooting," describes basic troubleshooting procedures.

Appendix A, "Connecting to the Cisco 3200 Series Router and Using the Command-Line Interface," describes how to use the command-line interface (CLI) to configure the WMIC.

Appendix B, "Channels and Antenna Settings," lists the WMIC radio channels and the maximum power levels supported by the world's regulatory domains.

Appendix C, "Protocol Filters," lists some of the protocols that you can filter on the WMIC.

Appendix D, "MIB List," lists the Simple Network Management Protocol (SNMP) Management Information Bases (MIBs) that the WMIC supports.

Appendix E, "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 fisicos. 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 Documentation

You can access these documents on the Documentation page on Cisco Connection Online (CCO) at www.cisco.com. The following documentation is available at the http://www.cisco.com/en/US/products/hw/routers/ps272/tsd_products_support_series_home.html URL:

- *Release Notes for the Cisco 3200 Series Mobile Access Routers*—Provides information on accessing documentation and technical assistance for the Cisco 3200 Series Mobile Access Router.
- *Cisco IOS Command Reference for Cisco Access Points and Bridges*[1]—New and revised Cisco IOS commands for the radio ports provided on the Wireless Mobile Interface Card (WMIC).
- *Cisco 3200 Series Wireless MIC Software Configuration Guide*[1]—Example procedures for using the IOS commands to configure the Wireless Mobile Interface Card (WMIC).
- *Configuration Guide for the Cisco 3200 Series Mobile Access Router*[1]—Example procedures for using the IOS commands to configure assembled Cisco 3200 Series routers.
- *Cisco 3200 Series Mobile Access Router Hardware Reference*[1]—This document. It provides descriptions of the Cisco MIC I/O cards found in Cisco 3200 Series routers.
- *Cisco 3200 Series Mobile Access Router Reference Sell Document*[1]—An overview of the reference sell program and components for the Cisco 3200 Series router.

The Release Notes for the Cisco 3250 Mobile Router lists the enhancements to and caveats for Cisco IOS releases as they relate to the Cisco 3200 Series router can be found at:

http://www.cisco.com/en/US/products/sw/iosswrel/products_ios_cisco_ios_software_releases.html or

http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/ps4629/index.html

[1] Also available on the platform-specific CD-ROM.

This feature adds support for RFC 2006 Set operations and security violation traps. For specifications, see RFC 2006, *The Definitions of Managed Objects for IP Mobility Support Using SMIv2.*

For information about using Cisco IOS software to configure SNMP, refer to the following documents:

- The "Configuring SNMP Support" chapter of the *Cisco IOS Configuration Fundamentals Configuration Guide,* Release 12.2
- The "SNMP Commands" chapter of the *Cisco IOS Configuration Fundamentals Command Reference,* Release 12.2

For information about using Cisco IOS software to configure SNMP MIB features, refer to the appropriate documentation for your network management system.

For information on configuring Mobile IP using Cisco IOS software, refer to the following documents:

- The "Configuring Mobile IP" chapter of the *Cisco IOS IP Configuration Guide,* Release 12.2
- The "Mobile IP Commands" chapter of the *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services,* Release 12.2

Related documents from the Cisco TAC Web pages include:

- *Antenna Cabling* (http://www.cisco.com/warp/public/102/wlan/antcable.html)

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 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

Ordering Documentation

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/index.shtml

- 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.

Tools and Web Sites

If you are registered Cisco Direct Customer, you can access the following web sites:

IOS Command Lookup—A search engine dedicated to finding information on Cisco IOS commands in the Cisco IOS Command Reference, Cisco IOS Configuration Guide, Catalyst Command Reference, and PIX Firewall Command Reference.

http://www.cisco.com/cgi-bin/Support/Cmdlookup/home.pl

Bug Toolkit—Searches for known bugs based on software version, feature set and keywords. The resulting matrix shows when each bug was integrated, or fixed if applicable.

http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

Feature Navigator—Locates the Cisco IOS Software release based on the features you want to run on your network.

http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp

Obtain information on compatibility between hardware products and software releases at the following public URL:

http://tools.cisco.com/Support/Fusion/FusionHome.do

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/

- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

  http://cisco.com/univercd/cc/td/doc/pcat/

- *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

Cisco 3200 Documentation CD

The *Cisco 3200 Series Router Documentation CD* contains the technical publications for the Cisco 3200 Series Mobile Access Router. To view the documentation requires Acrobat Reader 4.0 or higher.

After the CD is inserted in the CD ROM drive and recognized by your PC, do the following:

Step 1 Access the root directory CD drive.

Step 2 Double click the StartHere.htm file.

System Requirements for the CD

Processor	Pentium 150 MHz or faster recommended
PC Operating System	Microsoft Windows 95 Microsoft Windows 98 Microsoft Windows ME Microsoft Windows XP Microsoft Windows NT 4.0 Microsoft Windows 2000
Memory	64-MB DRAM
Drives	4x CD-ROM drive
Monitor	Color monitor capable of 800 x 600 pixel resolution
Software	Adobe Acrobat Reader 4.0 or later

Printing Documents from the CD

To print a document:

Step 1 Display the document in Acrobat.

Step 2 Click the **Printer** icon on the Acrobat toolbar.

The Windows Print Dialog box appears.

Step 3 Select your default printer, and click **OK**.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour-a-day, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance. If you do not hold a valid Cisco service contract, please contact your reseller.

Cisco TAC Website

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

http://www.cisco.com/tac

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

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

Opening a TAC Case

Using the online TAC Case Open Tool is the fastest way to open P3 and P4 cases. (P3 and P4 cases are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using the recommended resources, your case will be assigned to a Cisco TAC engineer. The online TAC Case Open Tool is located at this URL:

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

For P1 or P2 cases (P1 and P2 cases are those in which your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case 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 listing of Cisco TAC contacts, go to this URL:

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

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—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.

Priority 2 (P2)—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.

Priority 3 (P3)—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.

Priority 4 (P4)—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. Go to this URL to visit the company store:

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

- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

  http://cisco.com/univercd/cc/td/doc/pcat/

- *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 online at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. 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

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

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

Overview

The Cisco Wireless Mobile Interface Card (WMIC) provides wireless connectivity for the Cisco 3200 Series Mobile Access Router. WMICs operate in the 2.4-GHz or 4.9-GHz bands and conform to the 802.11 standards.

This chapter provides information on the following topics:

- Understanding the Cisco Mobile Wireless Network
- Features
- Management Options

Understanding the Cisco Mobile Wireless Network

This section provides basic wireless network configuration descriptions and an example of a metro mobile network. The 2.4-GHz WMIC has a fixed channel spacing and bandwidth of 20-MHz. The 4.9-GHz WMIC can be configured for different channel spacings or bandwidths of 5-MHz, 10-MHz, or 20-MHz. These channels are designed to be non overlapping and non-interfering.

Network Configuration Descriptions

This section describes the role of a Cisco 3200 Series Mobile Access Router in common wireless configurations: access point mode, point-to-point bridging, point-to-multipoint bridging, redundant bridging, and workgroup bridge mode.

Root Bridge–accepts associations from workgroup bridges, non-root bridges, and clients

Root Access Point–accepts assocations from workgroup bridge and clients

Workgroup Bridge–associates to root access points or root bridges

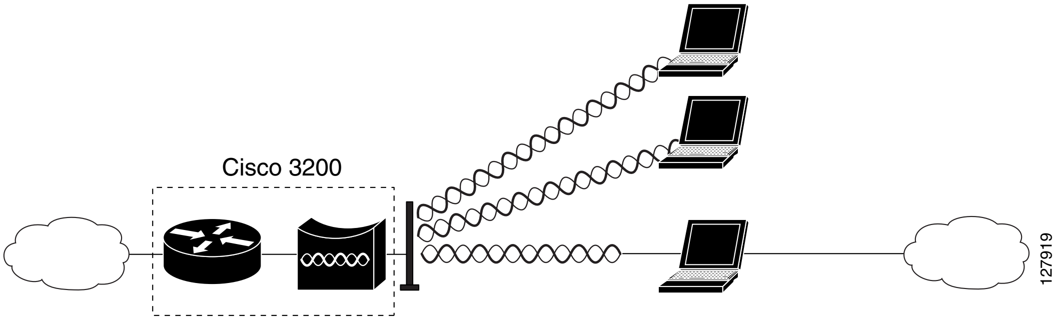
Non-Root Bridge–associates to root bridges

Access Point Mode

You can configure the WMIC as an access point. In the access point mode, the WMIC accepts associations from local client devices. See Chapter 4, "Configuring Radio Settings," for instructions on configuring the WMIC as an access point.

Figure 1-1 shows a typical scenario where the WMIC functions as an access point.

Figure 1-1 Access Point Mode

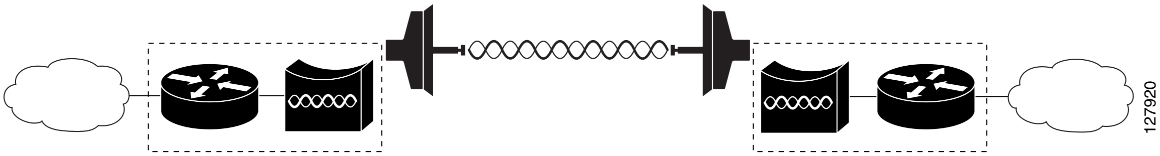


Point-to-Point Bridging

In a point-to-point configuration, a non-root bridge associates to a root bridge. The WMIC listens for another bridge. If it does not recognize another bridge, the WMIC becomes a root bridge. If it recognizes another bridge, it becomes a non-root bridge associated to the bridge it recognizes.

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

Figure 1-2 Point-to-Point Bridge Configuration

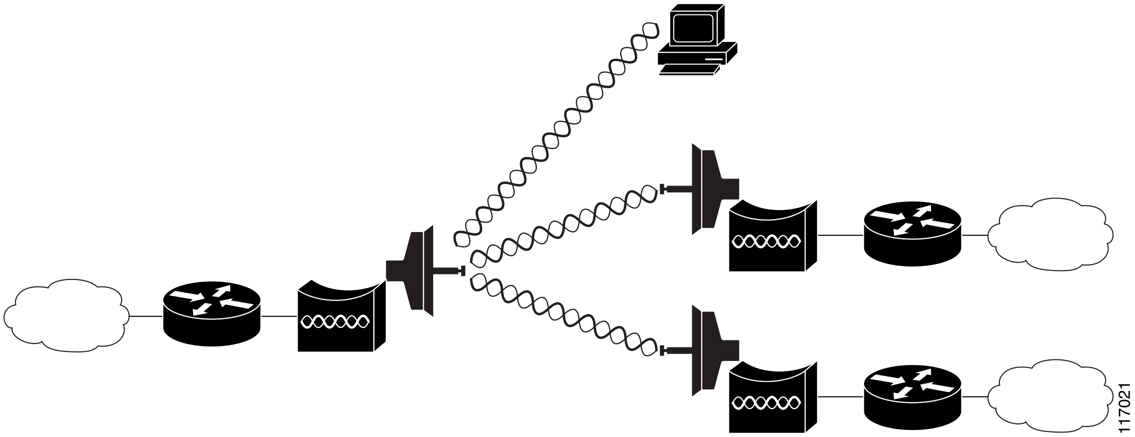


Point-to-Multipoint Bridging

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.

Figure 1-3 shows bridges in a point-to-multipoint configuration.

Figure 1-3 Point-to-Multipoint Configuration

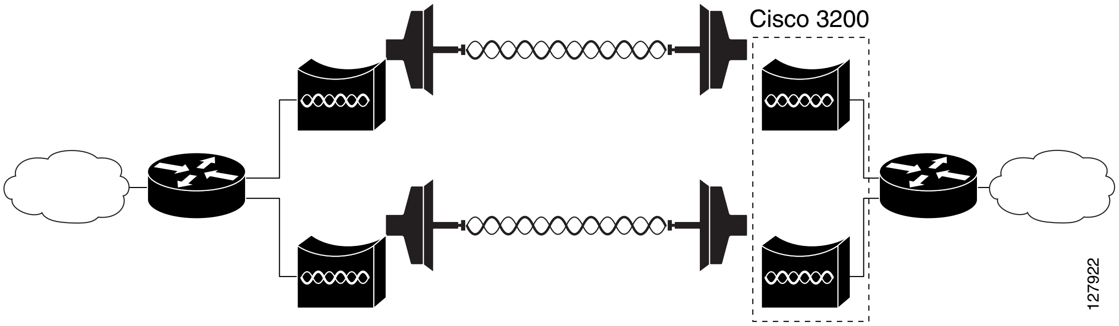


Redundant Bridging

You can set up two pairs of bridges to add redundancy or load balancing to the 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 loops. (STP is disabled by default. See Chapter 6, "Configuring Spanning Tree Protocol," for instructions on configuring STP.)

Figure 1-4 shows two pairs of redundant bridges.

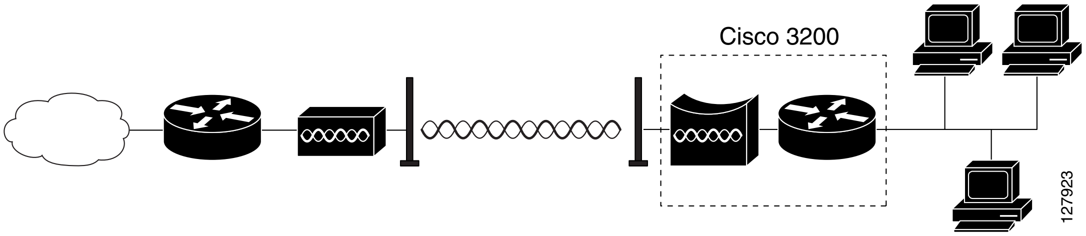
Figure 1-4 Redundant Bridge Configuration



Workgroup Bridge Mode

You can configure the WMIC to function as a workgroup bridge. Figure 1-5 shows a typical scenario where the WMIC functions as a workgroup bridge. See Chapter 4, "Configuring Radio Settings," for instructions on how to configure the WMIC as a workgroup bridge.

Figure 1-5 Workgroup Bridge Mode



Features

Cisco wireless devices running Cisco IOS offer these software features:

- VLANs—Allow VLAN trunking on both wireless and Ethernet interfaces.
- QoS—Use this feature to support quality of service for prioritizing traffic on the wireless interface.
- RADIUS Accounting—Enable accounting on the WMIC 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 WMIC.

- Enhanced security—Enable three advanced security features to protect against sophisticated attacks on your wireless network's WEP keys: Message Integrity Check (MIC) and WEP key hashing. Enhanced security for WPA/TKIP is also available.
- Enhanced authentication services—Set up non-root bridges or workgroup bridges to authenticate to the network like other wireless client devices. After a network username and password for the non-root bridge or workgroup bridge are set, it authenticates to the network using Cisco Light Extensible Authentication Protocol (LEAP), and receives and uses dynamic WEP keys.
- Advanced Encryption Standard (AES) (only available on the 4.9-GHz WMIC)—This feature supports Advanced Encryption Standard-Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP). AES-CCMP is required for Wi-Fi Protected Access 2 (WPA2) and IEEE 802.11i wireless LAN security.
- Enhanced authentication for Cisco Centralized Key Management (CCKM).
- Fast, secure roaming of client devices, and radio management through wireless domain services (WDS) (See the "Configuring WDS, Fast Secure Roaming, and Radio Management" chapter for more information.

Note The 4.9-GHz WMIC does not support CKIP and CMIC encryption; however, The 2.4-GHz WMIC does support CKIP and CMIC encryption.

The key differences between the 2.4-GHz WMIC and the 4.9-GHz WMIC are shown in Table 1-1.

Table 1-1 Differences Between the 2.4-GHz WMIC and the 4.9-GHz WMIC

Feature	*2.4-GHz WMIC*	*4.9-GHz WMIC*	Comment
Cookie and Banner	C3201	C32XX	
Frequency	2.4 GHz	4.9 GHz	
Data rates	802.11b data rates are 1 Mbps, 2 Mbps, 5.5 Mbps and 11 Mbps. 802.11g, data rates are 1 Mbps, 2 Mbps, 5.5 Mbps, 6 Mbps, 9 Mbps, 11 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps, and 54 Mbps	20-MHz base band. 6 Mbps, 9 Mbps, 12 Mbps, 24 Mbps, 36 Mbps, 48 Mbps, and 56 Mbps. 10-MHz base band. Data rates are 3 Mbps, 4.5 Mbps, 6 Mbps, 9 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, and 27 Mbps. 5-MHz base band. Data rates are 1.5 Mbps, 2.25 Mbps, 3 Mbps, 4.5 Mbps, 6 Mbps, 9 Mbps, 12 Mbps, and 13.5 Mbps	The **dot11 interface speed** command manages data rates and only applies to the 4.9-GHz WMIC.
Power	Maximum OFDM power level is 15 dBm (30mw). This varies by country.	Maximum OFDM power level is 17 dBm (50mw). US only.	The **dot11 interface power** command is used to manage the power levels.
Concatenation	Supported	Not supported	

Table 1-1 Differences Between the 2.4-GHz WMIC and the 4.9-GHz WMIC

Feature	*2.4-GHz WMIC*	*4.9-GHz WMIC*	Comment
distance command (minimizes delay propagation)	Supported	Supported	Formula to minimize the delay propagation will be added to the **dot11 interface distance** command
World Mode	Supported	Not supported	
HTML-Based User Interface	Supported	Not supported	
VLAN	16 unencrypted VLANs 16 static key VLANs 16 dynamic key VLANs	16 unencrypted VLANs 1 static key VLANs or 4 dynamic key VLANs	
Wireless encryption/cipher suites	WEP-40, WEP-128, TKIP, CKIP, CMIC, and CKIP-CMIC	WEP-40, WEP-128, TKIP, and AES-CCM	CKIP, CMIC and CKIP-CMIC are not part of 802.11 standard cipher suites.
Maximum number of stations with WEP	255	116	
Maximum number of stations with TKIP	256	26	
Maximum number of stations with AES-CCM	256	116	
Channelization	Statically declared as defined by IEEE 802.11b/g.	Channel spacing selected by using the CLI.	
WDS server	Not supported	Can be configured to act as WDS server.	
WDS client	2.4 GHz WMIC (C3201-WMIC) acting as Root device can auto-discover a WDS server.	Acting as Root device, it can auto-discover and work within a subnet WDS server.	If the IP address of a WDS server is statically configured, the 4.9-GHz WMIC, acting as Root device, can also work with central WDS server located anywhere in the network.

Table 1-1 Differences Between the 2.4-GHz WMIC and the 4.9-GHz WMIC

Feature	*2.4-GHz WMIC*	*4.9-GHz WMIC*	Comment
Scanning Enhancements for Faster Roaming	All *Scanning Enhancements for Faster Roaming* are available.	All *Scanning Enhancements for Faster Roaming* are available except "Use First Better Access Point."	• Synthesizer tuning time • Start on Current Channel • Only Probe Current SSID • Shorten Wait time for Probe Response • Automatically Limiting Frequencies Scanned • Time out the Scan • Use First Better Access Point • Save Best Probe Response
EAP-TLS, EAP-TTLS	Supported on root devices	Not supported	
SNMP MIB Ids	Supported	Supported (new values)	The platform-dependent SNMP code was modified to return new values. (entPhysicalVendorType, System OID, and Chassis ID)
Dot11 MIB parameters	Not available	The dot11 parameters are returned through the dot11 MIB interface.	
WDS server-related MIBS	Not available	Supported	

Management Options

You can use the WMIC management system through the following interfaces:

- The IOS command-line interface (CLI), which you use through a PC running terminal emulation software or a Telnet session. Appendix A, "Connecting to the Cisco 3200 Series Router and Using the Command-Line Interface," provides a detailed description of how the CLI is used to confugure the router. The "Preface" describes the command formats.
- Simple Network Management Protocol (SNMP). Chapter 14, "Configuring SNMP," explains how to configure your bridge for SNMP management.

Configuring the WMIC for the First Time

This chapter describes how to configure basic settings on a Wireless Mobile Interface Card (WMIC) 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 web-browser interface to complete the initial configuration and use the CLI to enter additional settings for a more detailed configuration.

This chapter contains these sections:

- Before You Start
- Connecting to the WMIC
- Obtaining and Assigning an IP Address
- Obtaining and Assigning an IP Address
- Configuring Basic Security Settings
- Using the IP Setup Utility

Before You Start

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

- A system name for the WMIC
- The case-sensitive wireless service set identifier (SSID) that your WMICs use
- If not connected to a DHCP server, a unique IP address for your WMIC (such as 172.17.255.115)
- If the WMIC 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)

Connecting to the WMIC

To configure the WMIC locally (without connecting the WMIC to a wired LAN), connect a PC to the console port. If the WMIC has an IP address and Telnet is allowed on the device, connect to a Fast Ethernet Switch Mobile Interface Card (FESMIC) Ethernet port by using an Ethernet cable, and use Telnet to establish the connection. Or you can Telnet into the WMIC from a node on the LAN.

Note When you connect your PC to the WMIC or reconnect your PC to the LAN, it might be necessary to release and renew the IP address on the PC. On most PCs, release and renew the IP address by rebooting the PC or by entering the **ipconfig /release** and **ipconfig /renew** commands in a command window. Consult your PC operating instructions for detailed instructions.

Using the Console Port to Access the Exec

Connect a PC to the WMIC console port by using a DB-9 to RJ-45 serial cable. Note that there might be several console ports on a Cisco 3200 Series router.

Follow these steps to access the CLI by connecting to the WMIC console port:

Step 1 Connect a nine-pin, female DB-9 to RJ-45 serial cable to the WMIC RJ-45 serial port on the router and to the COM port on your PC.

Step 2 Set up a terminal emulator to communicate with the WMIC. 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 WMIC 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 WMIC.

Using a Telnet Session to Access the Exec

Follow these steps to access the WMIC CLI by using a Telnet session. The WMIC must have been previously configured to accept a Telnet session.

These steps are for a PC running Microsoft Windows with a Telnet terminal application. Check the 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 WMIC IP address.

Step 3 In the Host Name field, type the WMIC IP address and click **Connect**.

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 the WMIC for Secure Shell" section for instructions on setting up the WMIC for SSH access.

Obtaining and Assigning an IP Address

To browse to the WMIC Express Setup page, you must assign the WMIC IP address using one of the following methods:

- Use command when you connect to the WMIC locally. For detailed instructions, see the "Connecting to the WMIC" section of this document.
- 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 WMIC Media Access Control (MAC) address. Your network administrator will query the DHCP server using the MAC address to identify the IP address.
  - Use the Cisco IP Setup Utility (IPSU) to identify the assigned address. You can also use IPSU to assign an IP address to the WMIC if it did not receive an IP address from the DHCP server. 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/public/sw-center/sw-wireless.shtml
  - 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.

Assigning an IP Address By Using the Exec

The WMIC links to the network using a Bridge Group Virtual Interface (BVI) that it creates automatically. Instead of tracking separate IP addresses for the WMIC Ethernet and radio ports, the network uses the BVI.

Note The WMIC supports only one BVI. Configuring more than one BVI might cause errors in the WMIC ARP table.

When you assign an IP address to the WMIC 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 BVI:

	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** *address mask*	Assign an IP address and address mask to the BVI. **Note** If you are connected to the WMIC using a Telnet session, you lose your connection to the WMIC when you assign a new IP address to the BVI. To continue configuring the WMIC using Telnet, use the new IP address to open another Telnet session to the WMIC.

Assigning Basic Settings By Using the Web Browser

After you determine or assign the WMIC IP address, browse to the Express Setup page and perform an initial configuration:

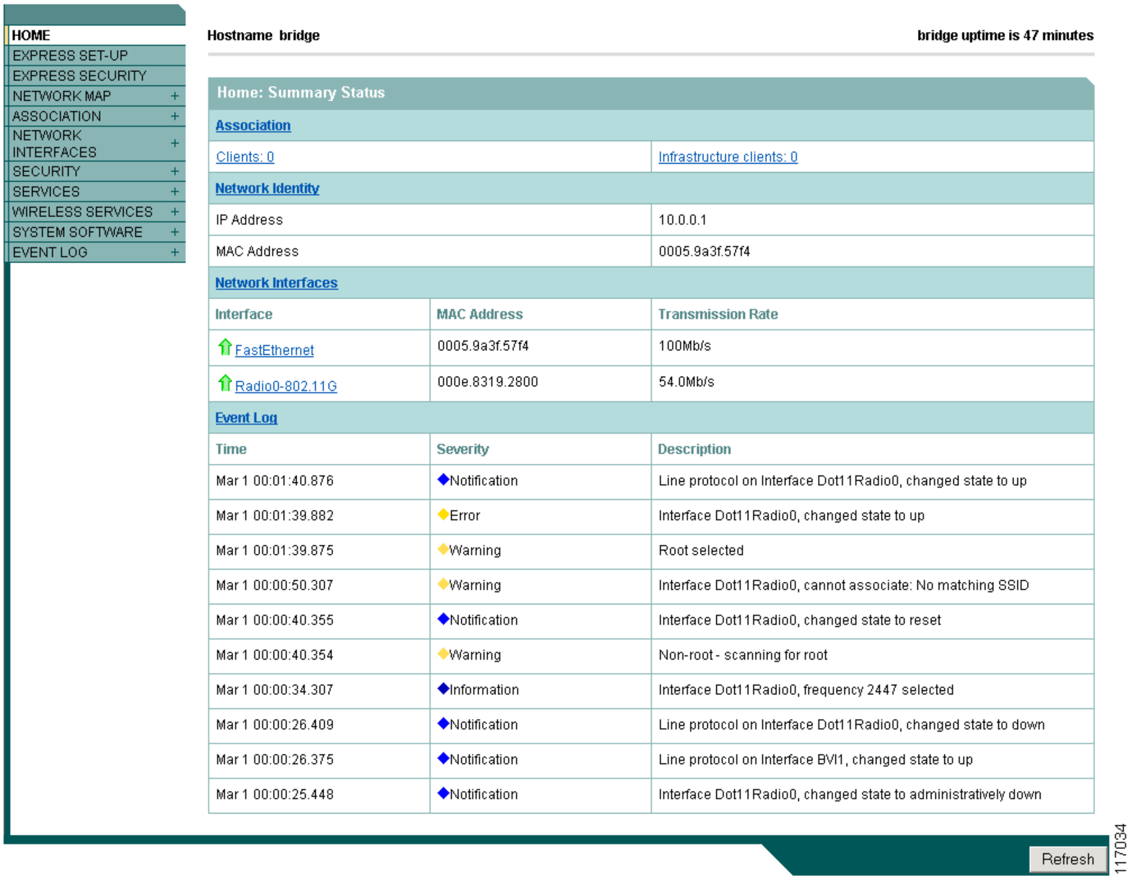
Step 1 Open your Internet browser. The web-browser interface is fully compatible with these browsers: Microsoft Internet Explorer versions 5.0, 5.01, 5.5 and 6.0; and Netscape Navigator versions 4.79 and 7.0.

Step 2 Enter the IP address in the browser address line and press **Enter**. An Enter Network Password screen appears.

Step 3 Press **Tab** to bypass the Username field and advance to the Password field.

Step 4 Enter the case-sensitive password (usually *Cisco)* and press **Enter**. The Summary Status page appears. Figure 2-1 shows the Summary Status page.

Figure 2-1 Summary Status 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

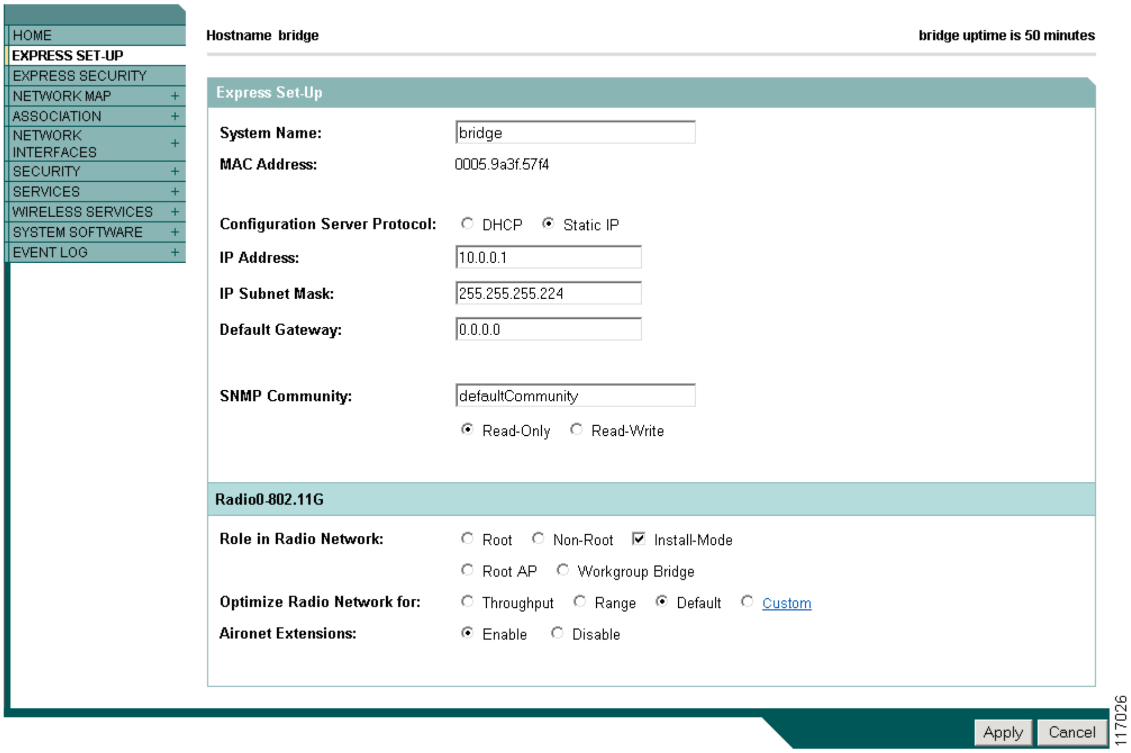
Interface	MAC Address	Transmission Rate
⇧ FastEthernet	0005.9a3f.57f4	100Mb/s
⇧ Radio0-802.11G	000e.8319.2800	54.0Mb/s

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

Step 5 Click **Express Setup**. The Express Setup screen appears. Figure 2-2 shows the Express Setup page.

Figure 2-2 Express Setup Page



Hostname bridge | bridge uptime is 50 minutes

Express Set-Up

System Name: bridge

MAC Address: 0005.9a3f.57f4

Configuration Server Protocol: ○ DHCP ● Static IP

IP Address: 10.0.0.1

IP Subnet Mask: 255.255.255.224

Default Gateway: 0.0.0.0

SNMP Community: defaultCommunity

● Read-Only ○ Read-Write

Radio0-802.11G

Role in Radio Network: ○ Root ○ Non-Root ☑ Install-Mode

○ Root AP ○ Workgroup Bridge

Optimize Radio Network for: ○ Throughput ○ Range ● Default ○ Custom

Aironet Extensions: ● Enable ○ Disable

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

- **System Name**— The system name, while not an essential setting, helps identify the WMIC on your network. The system name appears in the titles of the management system pages.
- **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 WMIC uses a static IP address that you enter in the IP address field.
- **IP Address**—Use this setting to assign or change the WMIC's IP address. If DHCP is enabled for your network, leave this field blank.

Note If the WMIC IP address changes while you are configuring the WMIC using the web-browser interface or a Telnet session over the wired LAN, you lose your connection to the WMIC. If you lose your connection, reconnect to the WMIC using its new IP address. Follow the steps in the "Obtaining and Assigning an IP Address" section on page 2-12 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 device on your network.
  - **Root—**Configures the device as a root bridge. In this mode, you establish a link with a non-root bridge. In this mode, the bridge also accepts associations from clients.
  - **Non-Root**— Places the device in non-root mode. In this mode, it links with a root bridge.
  - **Install Mode**—Places the device into installation mode so you can align and adjust the bridge link for optimum efficiency.
  - **Root AP**—Places the device in the access point mode. In this mode, the device accepts associations from client devices.
  - **Workgroup Bridge**—Places the device in the workgroup bridge mode. In this mode, the bridge accepts wired clients.

Note 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 or customized settings for the bridge radio. See the "Configuring the Radio Distance Setting" section on page 4-14 for more information on data rates and throughput.
  - **Throughput**—Maximizes the data volume handled by the WMIC but might reduce its range. When you select **Throughput**, the WMIC sets all data rates to **basic**.
  - **Range**—Maximizes the WMIC's range but might reduce throughput. When you select **Range**, the WMIC sets the 6-Mbps rate to **basic** and the other rates to **enabled**.
  - **Default**—The WMIC retains default radio settings that are designed to provide good range and throughput for most bridges.
  - **Custom**—Takes you to the Network Interfaces: Radio-802.11G Settings page.
- **Aironet Extensions**—Enabled by default, click the **Disable** Aironet Extensions radio button, and click Apply. The change will not be made to the configuration if the device is in workgroup bridge mode. In root bridge and non-root bridge mode, an error message displays, indicating that Aironet Extensions should always be enabled in root or non-root mode.

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

Your WMIC 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
System Name	bridge
Configuration Server Protocol	DHCP
IP Address	Assigned by DHCP by default; if DHCP is disabled, the default setting is 10.0.0.1
IP Subnet Mask	Assigned by DHCP by default; if DHCP is disabled, the default setting is 255.255.255.224
Default Gateway	Assigned by DHCP by default; if DHCP is disabled, the default setting is 0.0.0.0
SNMP Community	defaultCommunity
Role in Radio Network	Install-Mode
Optimize Radio Network for	Default
Aironet Extensions	Enable

Protecting Your Wireless LAN

After you assign basic settings to your WMIC, you must configure security settings to prevent unauthorized access to your network. Because it is a radio device, the WMIC 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 WMIC. Advanced security features can be found in the following chapters:

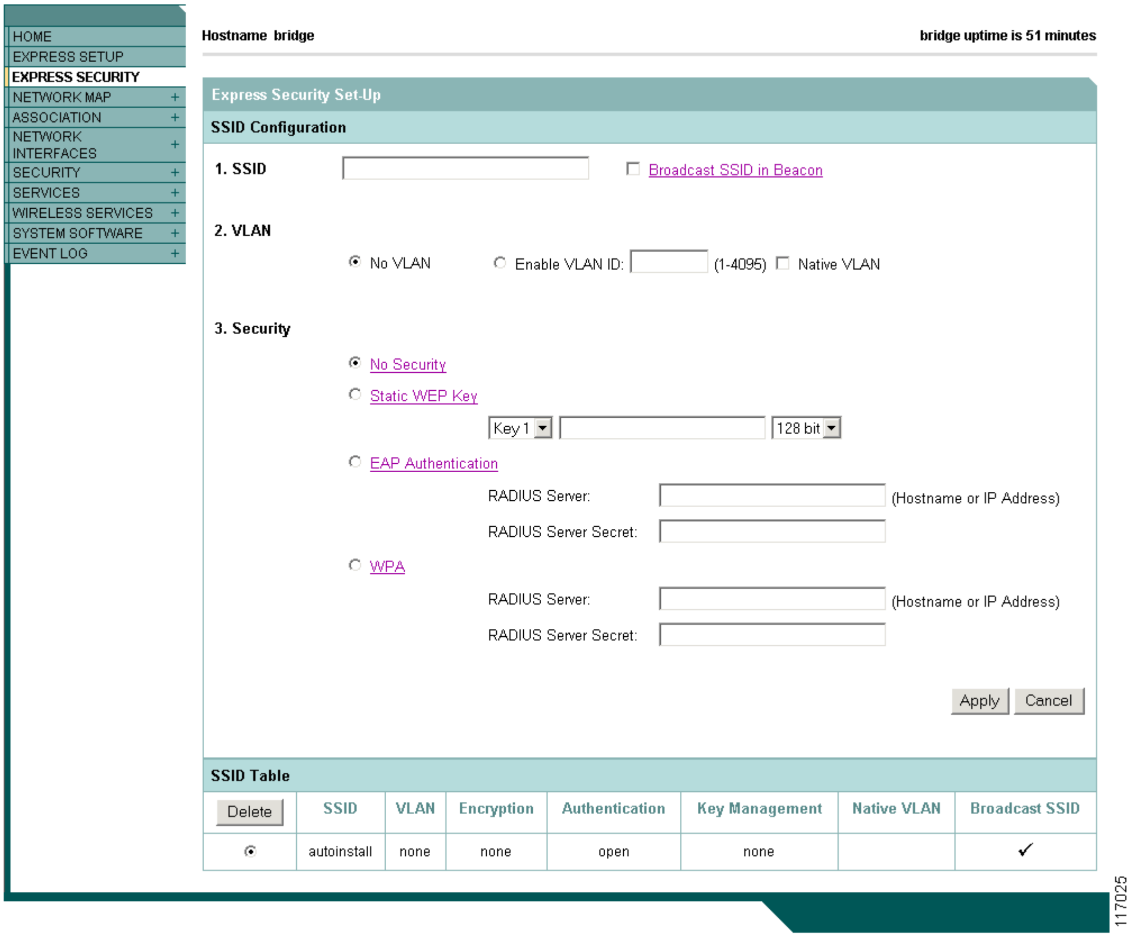
- A unique SSID that are not broadcast in the beacon (see Chapter 5, “Configuring SSIDs”
- WEP and WEP features (see Chapter 7, “Configuring WEP and WEP Features”)
- Dynamic WEP and WMIC authentication (see Chapter 8, “Configuring Authentication Types”)

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 2-3 shows the Express Security page.

Figure 2-3 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
●	autoinstall	none	none	open	none		✓

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

When the WMIC configuration is at factory defaults, the first SSID that you create using the Express security page overwrites the default SSID, *install*, which has no security settings. The SSIDs that you create appear in the SSID table at the bottom of the page. You can create up to 16 SSIDs on the access point.

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 WMIC's security capabilities. Keep these limitations in mind when using the Express Security page:

- 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 WMIC. 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.

a. The **Broadcast SSID in Beacon** setting is active only when the WMIC is in the Root AP mode. When you broadcast the SSID, devices that do not specify an SSID can associate to the WMIC 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 2 (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 3 (Optional) Check the Native VLAN check box to mark the VLAN as the native VLAN.

Step 4 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 2-18 for details.

Step 5 Click **Apply**. The SSID appears in the SSID table at the bottom of the page.

CLI Security 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 2-20
- Example: Static WEP, page 2-21
- Example: EAP Authentication, page 2-22
- Example: WPA, page 2-23

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
y
 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 IP address of a device when it has been assigned by a DHCP server. You can also use IPSU to set the IP address and SSID of a device if they have not been changed from the default settings. This section explains how to download the utility from Cisco.com and install it, how to use it to find the IP address of a device, and how to use it to set the IP address and the SSID.

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/public/sw-center/sw-wireless.shtml

Step 2 Click **Cisco Aironet Wireless LAN Client Adapters**.

Step 3 Scroll down to the Windows Utility section.

Step 4 Click **Cisco Aironet Client Utility (ACU) for Windows**.

Step 5 Click the file **IPSUvxxxxxx.exe**. The *vxxxxxx* identifies the software package version number.

Step 6 Read and accept the terms and conditions of the Software License Agreement.

Step 7 Download and save the file to a temporary directory on your hard drive and then exit the Internet browser.

Step 8 Double-click **IPSUvxxxxxx.exe** in the temporary directory to expand the file.

Step 9 Double-click **Setup.exe** and follow the steps provided by the installation wizard to install IPSU.

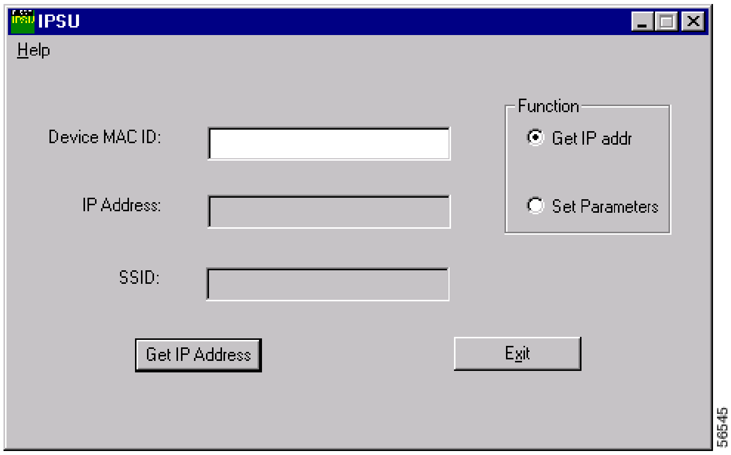
The IPSU icon appears on your computer desktop.

Using IPSU to Find the WMIC IP Address

If your WMIC 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 MAC address, you must run IPSU from a computer on the same subnet as the WMIC. Follow these steps to find the IP address:

Step 1 Double-click the **IPSU** icon on your computer desktop to start the utility. The IPSU screen appears (see Figure 2-4).

Figure 2-4 IPSU Get IP Address Screen



Function
● Get IP addr
○ Set Parameters

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 WMIC MAC address in the Device MAC ID field. The WMIC MAC address should contain six pairs of hexadecimal digits. The 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 IP address appears in the IP Address field, write it down.

If IPSU reports that the IP address is the default IP address, the WMIC did not receive a DHCP-assigned IP address. To change the IP address by using IPSU, refer to the "Using IPSU to Set the IP Address and SSID" section.

Using IPSU to Set the IP Address and SSID

To change the IP address of the WMIC, use IPSU. You can also set the SSID.

Note IPSU can change the IP address and SSID only from the default settings. After the IP address and SSID have been changed, IPSU cannot be used to change them again.

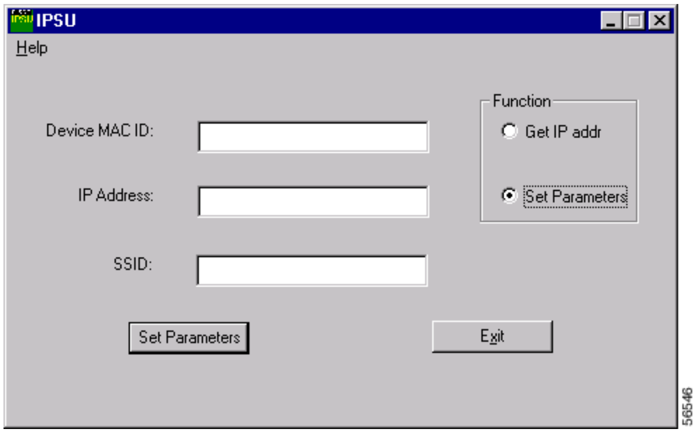
Note The computer you use to assign an IP address to the WMIC must have an IP address in the same subnet as the WMIC.

Follow these steps to assign an IP address and an SSID to the WMIC:

Step 1 Double-click the **IPSU** icon on your computer desktop to start the utility.

Step 2 Click the **Set Parameters** radio button in the Function box (see Figure 2-5).

Figure 2-5 IPSU Set Parameters Screen



Step 3 Enter the WMIC MAC address in the Device MAC ID field. The MAC address should contain six pairs of hexadecimal digits. Your MAC address might look like this example:

004096xxxxxx

Note The MAC address field is not case-sensitive.

Step 4 Enter the IP address you want to assign to the WMIC in the IP Address field.

Step 5 Enter the SSID you want to assign to the WMIC in the SSID field.

Note You cannot set the SSID without also setting the IP address. However, you can set the IP address without setting the SSID.

Step 6 Click **Set Parameters** to change the WMIC's IP address and SSID settings.

Step 7 Click **Exit** to exit IPSU.

Administering the WMIC

This chapter describes how to administer your WMIC. This chapter contains these sections:

- Configuring a System Name and Prompt
- Managing the System Time and Date
- Creating a Banner
- Protecting Access to Privileged EXEC Commands
- Protecting the Wireless LAN
- Controlling WMIC Access with RADIUS
- Controlling WMIC Access with TACACS+
- Configuring the WMIC for Local Authentication and Authorization
- Configuring the WMIC for Secure Shell
- Managing Aironet Extensions

Configuring a System Name and Prompt

You configure the system name on the WMIC to identify it. 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 12.1*.

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** *name*	Manually configure a system name. The default setting is *bridge*. 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.

Managing 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 WMIC, 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.

Default DNS Configuration

Table 3-1 shows the default DNS configuration.

Table 3-1 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 WMIC to use the DNS:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ip domain-name** *name*	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 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** *server-address1* [*server-address2 ... server-address6*]	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 WMIC 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 WMIC. 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.
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 WMIC 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 WMIC, 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*.

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 WMIC.

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** *c message c*	Specify the message of the day. For *c*, 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 *message*, enter a banner message up to 255 characters. You cannot use the delimiting character in the message.

	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.

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

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

```
bridge(config)# banner motd #
This is a secure site. Only authorized users are allowed.
For access, contact technical support.
#
bridge(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** *c message c*	Specify the login message. For *c*, 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 *message*, 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 WMIC using the dollar sign ($) symbol as the beginning and ending delimiter:

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

Managing the System Time and Date

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

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*.

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 3-17.

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.

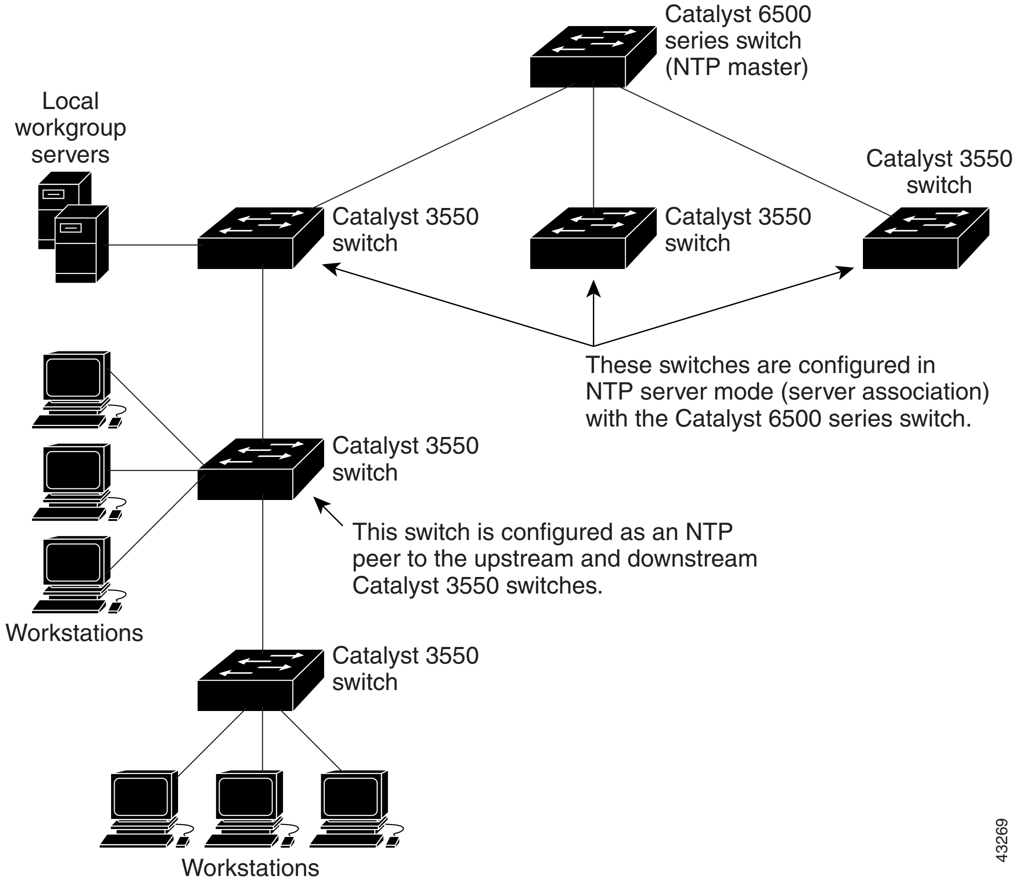
Cisco’s implementation of NTP does not support stratum 1 service; it is not possible to connect to a radio or atomic clock. We recommend that the time service for your network be derived from the public NTP servers available on the IP Internet. Figure 3-1 shows a typical network example using NTP.

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 3-1 Typical NTP Network Configuration


Catalyst 6500 series switch (NTP master)
Local workgroup servers
Catalyst 3550 switch
Catalyst 3550 switch
Catalyst 3550 switch
These switches are configured in NTP server mode (server association) with the Catalyst 6500 series switch.
Catalyst 3550 switch
This switch is configured as an NTP peer to the upstream and downstream Catalyst 3550 switches.
Workstations
Catalyst 3550 switch
Workstations
43269

Configuring NTP

WMICs 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 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.

Default NTP Configuration

Table 3-2 shows the default NTP configuration.

Table 3-2 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 WMIC 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.
Step 3	**ntp authentication-key** *number* **md5** *value*	Define the authentication keys. By default, none are defined. • For *number*, 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 *value*, enter an arbitrary string of up to eight characters for the key. The WMIC 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** *key-number* command.

	Command	Purpose
Step 4	**ntp trusted-key** *key-number*	Specify one or more key numbers (defined in Step 3) that a peer NTP device must provide in its NTP packets for this WMIC to synchronize to it. By default, no trusted keys are defined. For *key-number*, specify the key defined in Step 3. This command provides protection against accidentally synchronizing the WMIC 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 WMIC to synchronize only to devices providing authentication key 42 in the device's NTP packets:

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

Configuring NTP Associations

An NTP association can be a peer association (this WMIC 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 WMIC 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** *ip-address* [**version** *number*] [**key** *keyid*] [**source** *interface*] [**prefer**] or **ntp server** *ip-address* [**version** *number*] [**key** *keyid*] [**source** *interface*] [**prefer**]	Configure the WMIC system clock to synchronize a peer or to be synchronized by a peer (peer association). or Configure the WMIC system clock to be synchronized by a time server (server association). No peer or server associations are defined by default. • For *ip-address* 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 *number*, specify the NTP version number. The range is 1 to 3. By default, version 3 is selected. • (Optional) For *keyid*, enter the authentication key defined with the **ntp authentication-key** global configuration command. • (Optional) For *interface*, 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 WMIC to synchronize its system clock with the clock of the peer at IP address 172.16.22.44 using NTP version 2:

```
bridge(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 WMIC 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 WMIC can send NTP broadcast packets to a peer so that the peer can synchronize to it. The WMIC 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 WMIC to send NTP broadcast packets to peers so that they can synchronize their clock to the WMIC:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter interface configuration mode, and specify the interface to send NTP broadcast packets.
Step 3	**ntp broadcast** [**version** *number*] [**key** *keyid*] [*destination-address*]	Enable the interface to send NTP broadcast packets to a peer. By default, this feature is disabled on all interfaces. • (Optional) For *number*, specify the NTP version number. The range is 1 to 3. If you do not specify a version, version 3 is used. • (Optional) For *keyid*, specify the authentication key to use when sending packets to the peer. • (Optional) For *destination-address*, specify the IP address of the peer that is synchronizing its clock to this WMIC.
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:

```
bridge(config)# interface gigabitethernet0/1
bridge(config-if)# ntp broadcast version 2
```

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

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	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** *microseconds*	(Optional) Change the estimated round-trip delay between the WMIC 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:

```
bridge(config)# interface gigabitethernet0/1
bridge(config-if)# ntp broadcast client
```

Configuring NTP Access Restrictions

You can control NTP access by using access lists.

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-onl**y | **serve** | **peer**} *access-list-number*	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 WMIC to synchronize to the remote device. • **peer**—Allows time requests and NTP control queries and allows the WMIC to synchronize to the remote device. For *access-list-number*, enter a standard IP access list number from 1 to 99.
Step 3	**access-list** *access-list-number* **permit** *source* [*source-wildcard*]	Create the access list. • For *access-list-number*, enter the number specified in Step 2. • Enter the **permit** keyword to permit access if the conditions are matched. • For *source*, enter the IP address of the device that is permitted access to the WMIC. • (Optional) For *source-wildcard*, 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 WMIC 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 WMIC 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 WMIC NTP services, use the **no ntp access-group** {**query-only** | **serve-only** | **serve** | **peer**} global configuration command.

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

```
bridge# configure terminal
bridge(config)# ntp access-group peer 99
bridge(config)# ntp access-group serve-only 42
bridge(config)# access-list 99 permit 172.20.130.5
bridge(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** *interface-id*	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 WMIC 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** *type number*	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 3-11.

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 12.1*.

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 WMIC can synchronize, you do not need to manually set the system clock.

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** *hh***:***mm***:***ss day month year* or **clock set** *hh***:***mm***:***ss month day year*	Manually set the system clock using one of these formats. • For *hh***:***mm***:***ss*, specify the time in hours (24-hour format), minutes, and seconds. The time specified is relative to the configured time zone. • For *day*, specify the day by date in the month. • For *month*, specify the month by name. • For *year*, 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:

```
bridge# 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** *zone hours-offset* [*minutes-offset*]	Set the time zone. The device 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 *zone*, enter the name of the time zone to be displayed when standard time is in effect. The default is UTC. • For *hours-offset*, enter the hours offset from UTC. • (Optional) For *minutes-offset*, enter the minutes offset from UTC.
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** [*week day month hh***:***mm week day month hh***:***mm* [*offset*]]	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 *zone*, specify the name of the time zone (for example, PDT) to be displayed when summer time is in effect. • (Optional) For *week*, specify the week of the month (1 to 5 or **last**). • (Optional) For *day*, specify the day of the week (Sunday, Monday...). • (Optional) For *month*, specify the month (January, February...). • (Optional) For *hh***:***mm*, specify the time (24-hour format) in hours and minutes. • (Optional) For *offset*, 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:

```
bridge(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 *zone*, specify the name of the time zone (for example, PDT) to be displayed when summer time is in effect. • (Optional) For *week*, specify the week of the month (1 to 5 or **last**). • (Optional) For *day*, specify the day of the week (Sunday, Monday...). • (Optional) For *month*, specify the month (January, February...). • (Optional) For *hh*:*mm*, specify the time (24-hour format) in hours and minutes. • (Optional) For *offset*, 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
```

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. Default Password and Privilege Level Configuration

Table 3-3 shows the default password and privilege level configuration.

Table 3-3 Default Password and Privilege Levels

Feature	Default Setting
Username and password	Default username is *Cisco* and the default password is *Cisco*.
Enable password and privilege level	Default password is *Cisco*. 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 *Cisco*. 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 *Cisco*. 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** *password*	Define a new password or change an existing password for access to privileged EXEC mode. The default password is *Cisco*. For *password*, 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 Crtl-V when you create the password; for example, to create the password abc?123, do this: 1. Enter **abc**. 2. Enter **Crtl-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 WMIC configuration file.

This example shows how to change the enable password to *l1u2c3k4y5*. The password is not encrypted and provides access to level 15 (traditional privileged EXEC mode access):

```
bridge(config)# enable password l1u2c3k4y5
```

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** *level*] {*password* | *encryption-type encrypted-password*}
	or
	enable secret [**level** *level*] {*password* | *encryption-type encrypted-password*}
		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 *level*, 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 *password*, 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 *encryption-type*, 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 WMIC 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 3-25.

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:

```
bridge(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 WMIC. These pairs are assigned to lines or interfaces and authenticate each user before that user can access the WMIC. 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** *name* [**privilege** *level*] {**password** *encryption-type password*}	Enter the username, privilege level, and password for each user. • For *name*, specify the user ID as one word. Spaces and quotation marks are not allowed. • (Optional) For *level*, 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 *encryption-type*, enter 0 to specify that an unencrypted password will follow. Enter 7 to specify that a hidden password will follow. • For *password*, specify the password the user must enter to gain access to the WMIC. 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 WMIC. If you enter no username for the only username, you can be locked out of the WMIC.

Configuring Multiple Privilege Levels

By default, the 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.

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 *mode*, enter **configure** for global configuration mode, **exec** for EXEC mode, **interface** for interface configuration mode, or **line** for line configuration mode. • For *level*, 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 *command*, 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 *level*, the range is from 0 to 15. Level 1 is for normal user EXEC mode privileges. • For *password*, 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:

```
bridge(config)# privilege exec level 14 configure
bridge(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** *level*	Log in to a specified privilege level. For *level*, the range is 0 to 15.
Step 2	**disable** *level*	Exit to a specified privilege level. For *level*, the range is 0 to 15.

Protecting the Wireless LAN

Configure security settings to prevent unauthorized access to your network. Because it is a radio device, the WMIC can communicate beyond the physical boundaries of your building. Advanced security features can be found in the following chapters:

- A unique SSID that are not broadcast in the beacon (see Chapter 5, "Configuring SSIDs")
- WEP and WEP features (see Chapter 7, "Configuring WEP and WEP Features")
- Dynamic WEP authentication (see Chapter 8, "Configuring Authentication Types")

Using VLANs

Assign SSIDs to the VLANs on the wireless LAN. If you do not use VLANs on the wireless LAN, the security options that can be assigned to SSIDs are limited, because encryption settings and authentication types are linked. Without VLANs, encryption settings (WEP and ciphers) are applied to an interface and no more than one encryption setting can be used on each interface.

For example, if an SSID with static WEP is created with VLANs disabled, an additional SSIDs with WPA authentication cannot be created because of the different encryption settings. If a security setting for an SSID conflicts with another SSID, delete one or more SSIDs to eliminate the conflict.

Express Security Types

Table 3-4 describes the four security types that you can assign to an SSID.

Table 3-4 Security Types

Security Type	Description	Security Features Enabled
No Security	This is the least secure option. 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. Consider limiting association to the access point based on MAC address or, if the 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 access point mode, client devices cannot associate using this SSID without a WEP key that matches the access point key.
EAP Authentication	This option enables 802.1x authentication (such as LEAP, PEAP, EAP-TLS, EAP-GTC, EAP-SIM, and others) requires an IP address and shared secret for an authentication server on the network (server authentication port 1645). Because 802.1x authentication provides dynamic encryption keys, a WEP key is not required.	Mandatory 802.1x authentication, In root access point 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, the IP address and shared secret for an authentication server on your network (server authentication port 1645) are required.	Mandatory WPA authentication. In root access point mode, client devices that associate using this SSID must be WPA-capable.

Security Configuration Examples

This section contains these example configurations:

- No Security SSID Example
- Static WEP Security Example
- EAP Authentication Security Example
- WPA Security Example

No Security SSID Example

This example shows part of the configuration 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 (as it applies to the 2.4-GHz (802.11b/g) WMIC):

```
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
```

As it applies to the 4.9-GHz (US Only, Public Safety) WMIC:

```
hostname root
!
username Cisco password 7 02250D480809
ip subnet-zero
!
no aaa new-model
!
bridge irb
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 ssid test
    authentication open
    infrastructure-ssid
 !
 spacing 5 channel 4942
 speed basic-1.5 2.25 basic-3.0 4.5 basic-6.0 9.0 12.0 13.5
 power local 10
 station-role root
 infrastructure-client
 bridge-group 1
 bridge-group 1 spanning-disabled
!
interface FastEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 bridge-group 1 spanning-disabled
!
interface BVI1
 ip address 192.1.1.2 255.255.255.0
 no ip route-cache
!
ip http server
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
logging snmp-trap emergencies
logging snmp-trap alerts
logging snmp-trap critical
logging snmp-trap errors
logging snmp-trap warnings
bridge 1 route ip
!
!
!
line con 0
 exec-timeout 0 0
 transport preferred all
 transport output all
line vty 0 4
 login local
 transport preferred all
 transport input all
 transport output all
line vty 5 15
 login
 transport preferred all
 transport input all
 transport output all
!
end
```

Static WEP Security Example

This example shows part of the configuration 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-key
 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
```

EAP Authentication Security Example

This example shows part of the configuration 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
!
```

WPA Security Example

This example shows part of the configuration that creates 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
```

Configuring and Enabling RADIUS

This section describes how to configure and enable Remote Authentication Dial-In User Service (RADIUS).

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 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.

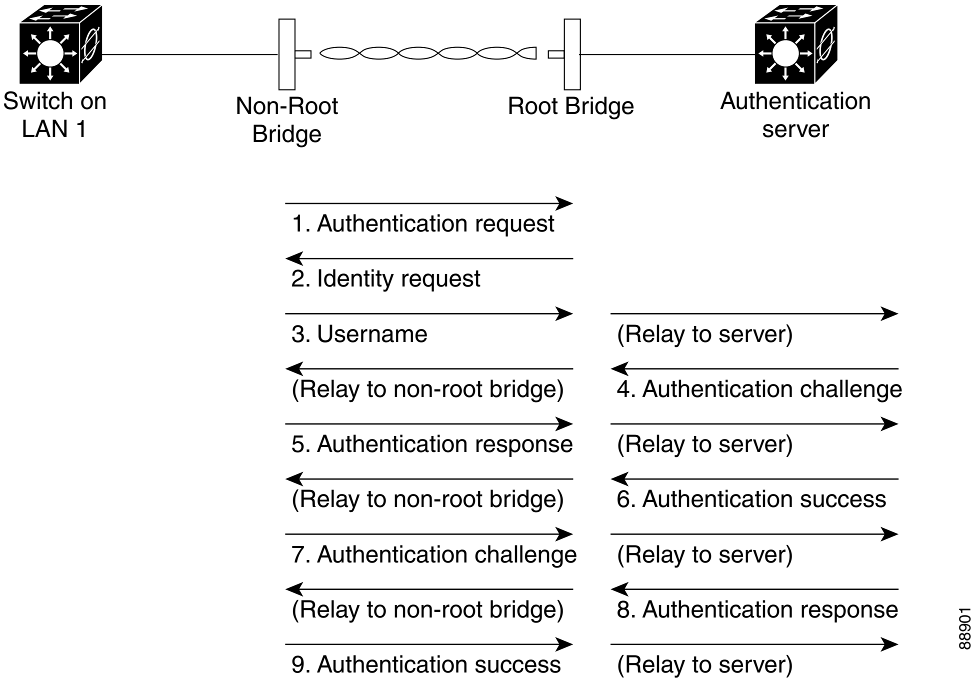
RADIUS is not suitable in these network security situations:

- 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 non-root bridge attempts to authenticate to a bridge whose access is controlled by a RADIUS server, authentication to the network occurs in the steps shown in Figure 3-2:

Figure 3-2 Sequence for EAP Authentication


Switch on LAN 1
Non-Root Bridge
Root Bridge
Authentication server
1. Authentication request
2. Identity request
3. Username
(Relay to server)
(Relay to non-root bridge)
4. Authentication challenge
5. Authentication response
(Relay to server)
(Relay to non-root bridge)
6. Authentication success
7. Authentication challenge
(Relay to server)
(Relay to non-root bridge)
8. Authentication response
9. Authentication success
(Relay to server)
88901

In Steps 1 through 9 in Figure 3-2, a non-root bridge and a RADIUS server on the wired LAN use 802.1x and EAP to perform a mutual authentication through the root bridge. The RADIUS server sends an authentication challenge to the non-root bridge. The non-root 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 bridge. When the RADIUS server authenticates the non-root bridge, the process repeats in reverse, and the non-root bridge authenticates the RADIUS server.

When mutual authentication is complete, the RADIUS server and the non-root bridge determine a WEP key that is unique to the non-root bridge and provides the non-root 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 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 bridge. The root bridge encrypts its broadcast key with the session key and sends the encrypted broadcast key to the non-root bridge, which uses the session key to decrypt it. The non-root bridge and the root 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 root bridge behaves the same way for each type: it relays authentication messages from the non-root bridge to the RADIUS server and from the RADIUS server to the non-root bridge. See the "Assigning Authentication Types to an SSID" section on page 8-6 for instructions on setting up authentication using a RADIUS server.

Controlling WMIC Access with RADIUS

This section describes how to control administrator access to the WMIC using RADIUS.

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. RADIUS and AAA are disabled by default.

At a minimum, the host or hosts that run the RADIUS server software must be identified and the method lists for RADIUS authentication must be defined. Optionally, method lists for RADIUS authorization and accounting can be defined.

A method list defines the sequence and methods to be used to authenticate, to authorize, or to keep accounts on a non-root bridge. Method lists are used 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 non-root bridges; 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 must have access to and should configure a RADIUS server before configuring RADIUS features.

These sections describe RADIUS configuration:

- Identifying the RADIUS Server Host
- Configuring RADIUS Login Authentication
- Defining AAA Server Groups
- Configuring RADIUS Authorization for User Privileged Access and Network Services
- Starting RADIUS Accounting
- Configuring Settings for All RADIUS Servers
- Configuring the Bridge to Use Vendor-Specific RADIUS Attributes
- Configuring the Bridge for Vendor-Proprietary RADIUS Server Communication
- Displaying the RADIUS Configuration

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*.

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

RADIUS security servers are identified by their host name or IP address, host name and specific UDP port numbers, or 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.

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 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 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 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 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 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 3-42.

You can configure the 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 3-39.

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** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]	Specify the IP address or host name of the remote RADIUS server host. • (Optional) For **auth-port** *port-number*, specify the UDP destination port for authentication requests. • (Optional) For **acct-port** *port-number*, specify the UDP destination port for accounting requests. • (Optional) For **timeout** *seconds*, specify the time interval that the 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** *retries*, 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** *string*, specify the authentication and encryption key used between the 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 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 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	**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 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:

```
bridge(config)# radius-server host 172.29.36.49 auth-port 1612 key rad1
bridge(config)# radius-server host 172.20.36.50 acct-port 1618 key rad2
```

This example shows how to configure *host1* as the RADIUS server and to use the default ports for both authentication and accounting:

```
bridge(config)# radius-server host host1
```

Configuring RADIUS Login Authentication

To configure AAA authentication, define a named list of authentication methods and 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 (in this case, a non-root bridge). 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.

	Command	Purpose
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 *not* 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 *method1...*, 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.
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 *list-name*, specify the list created with the **aaa authentication login** command.
Step 6	**radius-server attribute 32 include-in-access-req format %h**	Configure the device 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 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

Configure the bridge to use AAA server groups to group existing server hosts for authentication. 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.

Use the **server** group server configuration command to associate a particular server with a defined group server. 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.
Step 3	**radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]	Specify the IP address or host name of the remote RADIUS server host. • (Optional) For **auth-port** *port-number*, specify the UDP destination port for authentication requests. • (Optional) For **acct-port** *port-number*, specify the UDP destination port for accounting requests. • (Optional) For **timeout** *seconds*, specify the time interval that the 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** *retries*, 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** *string*, specify the authentication and encryption key used between the 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 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 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.

	Command	Purpose
Step 4	**aaa group server radius** *group-name*	Define the AAA server-group with a group name. This command puts the bridge in a server group configuration mode.
Step 5	**server** *ip-address*	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 3-37.

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 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.

```
bridge(config)# aaa new-model
bridge(config)# radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
bridge(config)# radius-server host 172.10.0.1 auth-port 1645 acct-port 1646
bridge(config)# aaa group server radius group1
bridge(config-sg-radius)# server 172.20.0.1 auth-port 1000 acct-port 1001
bridge(config-sg-radius)# exit
bridge(config)# aaa group server radius group2
bridge(config-sg-radius)# server 172.20.0.1 auth-port 2000 acct-port 2001
bridge(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 bridge uses information retrieved from the user 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 bridge for user RADIUS authorization for all network-related service requests.
Step 3	**aaa authorization exec radius**	Configure the 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 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.

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 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.

Configuring Settings for All RADIUS Servers

Beginning in privileged EXEC mode, follow these steps to configure global communication settings between the bridge and all RADIUS servers:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**radius-server key** *string*	Specify the shared secret text string used between the 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** *retries*	Specify the number of times the 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** *seconds*	Specify the number of seconds an 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** *minutes*	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, or unless there are no servers not marked dead. **Note** If you set up more than one RADIUS server, you must configure the RADIUS server deadtime for optimal performance.
Step 6	**radius-server attribute 32 include-in-access-req format %h**	Configure the 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 the retransmit, timeout, and deadtime, use the **no** forms of these commands.

Configuring the 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 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 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 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 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 Bridge for Vendor-Proprietary RADIUS Server Communication

Although an IETF draft standard for RADIUS specifies a method for communicating vendor-proprietary information between the 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 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.
Step 3	**radius-server key** *string*	Specify the shared secret text string used between the bridge and the vendor-proprietary RADIUS server. The 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 bridge and the server:

```
bridge(config)# radius-server host 172.20.30.15 nonstandard
bridge(config)# radius-server key rad124
```

Displaying the RADIUS Configuration

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

Controlling WMIC Access with TACACS+

This section describes how to control administrator access to the WMIC using Terminal Access Controller Access Control System Plus (TACACS+).

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*.

Understanding TACACS+

TACACS+ is a security application that provides centralized validation of users attempting to gain access to your bridge. Unlike RADIUS, TACACS+ does not authenticate non-root bridges associated to the root 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 WMIC.

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 WMIC and the TACACS+ daemon, and it ensures confidentiality because all protocol exchanges between the WMIC and the TACACS+ daemon are encrypted.

You need a system running the TACACS+ daemon software to use TACACS+ on your WMIC.

TACACS+ Operation

When an administrator attempts a simple ASCII login by authenticating to a WMIC using TACACS+, this process occurs:

1. When the connection is established, the WMIC contacts the TACACS+ daemon to obtain a username prompt, which is then displayed to the administrator. The administrator enters a username, and the WMIC then contacts the TACACS+ daemon to obtain a password prompt. The WMIC 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 WMIC eventually receives one of these responses from the TACACS+ daemon:
   - ACCEPT—The administrator is authenticated and service can begin. If the WMIC 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 WMIC. If an ERROR response is received, the WMIC 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 WMIC. 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

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 WMIC 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.

Identifying the TACACS+ Server Host and Setting the Authentication Key

You can configure the WMIC 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** *hostname* [**port** *integer*] [**timeout** *integer*] [**key** *string*]	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 *hostname*, specify the name or IP address of the host. • (Optional) For **port** *integer*, specify a server port number. The default is port 49. The range is 1 to 65535. • (Optional) For **timeout** *integer*, specify a time in seconds the WMIC 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** *string*, specify the encryption key for encrypting and decrypting all traffic between the WMIC 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+** *group-name*	(Optional) Define the AAA server-group with a group name. This command puts the WMIC in a server group subconfiguration mode.
Step 5	**server** *ip-address*	(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. 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 *not* 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 *list-name*, specify a character string to name the list you are creating. • For *method1...*, 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**] *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** | *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 *list-name*, 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 WMIC 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 WMIC for user TACACS+ authorization for all network-related service requests.
Step 3	**aaa authorization exec tacacs+**	Configure the WMIC 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).

	Command	Purpose
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 WMIC 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.
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 the WMIC for Local Authentication and Authorization

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

Beginning in privileged EXEC mode, follow these steps to configure the WMIC 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.
Step 6	**username** *name* [**privilege** *level*] {**password** *encryption-type password*}	Enter the local database, and establish a username-based authentication system. Repeat this command for each user. • For *name*, specify the user ID as one word. Spaces and quotation marks are not allowed. • (Optional) For *level*, 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 *encryption-type*, enter **0** to specify that an unencrypted password follows. Enter **7** to specify that a hidden password follows. • For *password*, specify the password the user must enter to gain access to the WMIC. 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 WMIC 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 12.2*.

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 only SSH version 1.

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 WMIC Access with RADIUS" section on page 3-34)
- Local authentication and authorization (for more information, see the "Configuring the WMIC for Local Authentication and Authorization" section on page 3-51)

For more information about SSH, refer to the "Configuring Secure Shell" section in the *Cisco IOS Security Configuration Guide for Release 12.2*.

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 information about configuring SSH and displaying SSH settings, refer to the “Configuring Secure Shell” section in the *Cisco IOS Security Configuration Guide for Release 12.2*.

Managing Aironet Extensions

The WMIC uses Cisco Aironet 802.11 extensions to detect the capabilities of Cisco client devices and to support features that require specific interaction between the WMIC and associated client devices. The Aironet Extensions can only be deactivated in the Root Access Point mode.   Since workgroup bridge, root bridge, and non-root bridge are Cisco-specific modes, they always use the Aironet extensions.

Aironet extensions must be enabled to support these features:

- Load balancing—The WMIC 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 WMIC 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.
- Limiting the power level on associated client devices—When a client device associates to the WMIC, the WMIC sends the maximum allowed power level setting to the client.

Beginning in privileged EXEC mode, follow these steps to disable the Aironet extensions:

	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 root ap-only**	Enter the station role. Root enables the access point mode.
Step 4	**no dot11 extension aironet**	Enter the **extension aironet** command to disable extensions.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

If you change the radio to a role that requires Aironet extensions, the Aironet extensions are enabled automatically:

```
wmic1(config)#int dot 0
wmic1(config-if)#station-role root
Selected role requires Cisco Aironet Extension enabled.
Enabled Cisco Aironet Extension.
```

If you try to change the Aironet extensions without setting the radio to the proper role, an error message displays:

```
wmic1(config-if)#
wmic1(config-if)#no dot11 extension aironet
Aironet Extension is always enabled in Bridge or WGB mode.
```

CHAPTER 4

Configuring Radio Settings

This chapter describes how to configure radio settings for your WMIC. This chapter includes these sections:

- Disabling and Enabling the Radio Interface
- Configuring the Role in Radio Network
- Configuring Radio Data Rates
- Configuring Radio Transmit Power
- Configuring Radio Channel Settings
- Enabling and Disabling World Mode (2.4-GHz Only)
- Disabling and Enabling Short Radio Preambles (2.4-GHz Only)
- Configuring Transmit and Receive Antennas
- Configuring the Ethernet Encapsulation Transformation Method
- Enabling and Disabling Concatenation (2.4-GHz Only)
- Configuring the Radio Distance Setting
- Enabling and Disabling Reliable Multicast to Workgroup Bridges
- Enabling and Disabling Public Secure Packet Forwarding
- Configuring the Beacon Period
- Configure RTS Threshold and Retries
- Configuring the Maximum Data Retries
- Configuring the Fragmentation Threshold
- Setting the Root Parent Timeout Value
- Configuring the Root Parent MAC
- Performing a Carrier Busy Test

Disabling and Enabling the Radio Interface

The WMIC radio is enabled by default. Beginning in privileged EXEC mode, follow these steps to disable the WMIC 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	**shutdown**	Disable the radio port.
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 shutdown command to enable the radio port.

Configuring the Role in Radio Network

You can configure your WMIC as a root bridge, non-root bridge, access point, or workgroup bridge. (Chapter 1, "Overview" describes the various WMIC radio network roles.) Beginning in privileged EXEC mode, follow these steps to set the WMIC 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.
Step 3	**station-role** {**root** [**ap-only**] | **non-root** | **workgroup-bridge** | **install** [**automatic** | **root** | **non-root**]}	Set the WMIC role. • **Bridge**—root, non-root, or install modes. In root mode, the access point function is automatically enabled allowing client devices to associate. • **Access point**—root ap-only mode • **Workgroup bridge**—workgroup bridge mode
Step 4	**mobile station**	(Optional) Use this command to configure a non-root bridge or workgroup bridge as a mobile station. When this feature is enabled the 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 WMIC 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 WMIC 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.

Configuring the WMIC as an Access Point

The WMIC can be configured as a root access point. In this role, it accepts associations from wireless clients.

Follow these steps to configure the WMIC as an access point:

	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 root ap-only**	Specifies that the WMIC functions as a root access point.
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 WMIC as a Workgroup Bridge

The WMIC can be configured as a workgroup bridge. In this role, the WMIC has the following functionality:

- Associates to the following devices:
  - Root access points
  - Root bridges
- If the router contains a 2.4-GHz WMIC, it operates with 2.4-GHz (802.11b/g) IOS-based bridges. If the router contains a 4.9-GHz WMIC, it operates with 4.9-GHz IOS-based bridges.
- Accepts only wired clients.
- Informs its root parent of all attached wired clients using IAPP messaging.

Follow these steps to configure the WMIC 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.
Step 3	**station-role workgroup-bridge**	Enables workgroup bridge mode.
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 WMIC as a Bridge

The WMIC can be configured as a bridge. This is the only role that supports the **distance** command.

There are three install modes: automatic, root, and non-root:

Automatic activates the bridge install and alignment mode, and specifies that the unit automatically determines the network role. If the unit is able to associate to another Cisco root bridge within 60 seconds, the unit assumes a non-root bridge role. If the unit is unable to associate with another Cisco root bridge within 60 seconds, the unit assumes a root bridge role. The device can be configured into root bridge or non-root bridge modes to avoid the 60-second automatic detection phase.

Root specifies that the device is operating as a root bridge and connects directly to the main Ethernet LAN network. In this mode, the unit accepts associations from other Cisco bridges and wireless client devices.

Non-root specifies that the device is operating as a non-root bridge, and that it connects to a remote LAN network, and that it must associate with a Cisco root bridge by using the wireless interface.

Follow these steps to configure the WMIC to determine is role automatically:

	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 install automatic**	Specifies that role of the WMIC is chosen based on the device to which it is associated.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Configuring Radio Data Rates

You use the data rate settings to choose the data rates the 4.9-GHz (US Only, Public Safety) WMIC uses for data transmission. The rates are expressed in megabits per second. The WMIC 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 WMIC 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 WMIC's data rates must be set to Basic.
- Enabled—The WMIC transmits only unicast packets at this rate; multicast packets are sent at one of the data rates set to Basic.
- Disabled—The WMIC 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 up the WMIC to operate at specific data rates. For example, to configure the WMIC to operate at 54 megabits per second (Mbps) service only, set the 54-Mbps rate to **Basic** and set the other data rates to **Enabled**. To set up the WMIC to operate at 24, 48, and 54 Mbps, set 24, 48, and 54 to **Basic** and set the rest of the data rates to **Enabled**.

You can also configure the WMIC to set the data rates automatically to optimize either range or throughput. When you enter **range** for the data rate setting, the WMIC sets the 6-Mbps rate to **basic** and the other rates to **enabled** if you are configuring a 2.4-GHz WMIC or a 4.9-GHz WMIC.

If you are configuring a 4.9-GHz WMIC set to 5-MHz spacing, the WMIC sets the 1.5- Mbps rate to **basic** and the other rates to **enable**. If you are configuring a 4.9-GHz WMIC set to 10-MHz spacing, the WMIC sets the 3.0-Mbps rate to **basic** and the other rates to **enable**. If you enter **throughput** for the data rate setting, the WMIC 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.
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** | **default** }	Set each data rate to **basic** or **enabled**, or enter **range** to optimize the range or **throughput** to optimize the throughput. If you are entering the speed for a 2.4-GHz WMIC, 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**. If you are entering the speed for a 4.9-GHz WMIC: With 5-MHz spacing, enter a speed of **1.5, 2.25, 3.0, 4.5, 6.0, 9.0, 12.0,** or **13.5**. With 10-MHz spacing, enter a speed of **3.0, 4.5, 6.0, 9.0, 12.0, 18.0, 24.0,** or **27.0**. 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**. **Note** The client must support the basic rate that you select or it cannot associate to the WMIC. 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 WMIC's 802.11g radio. • (Optional) Enter **range** or **throughput** to automatically optimize radio range or throughput. When you enter **range**, The WMIC sets the lowest data rate to basic and the other rates to **enabled**. When you enter **throughput**, the WMIC sets all data rates to **basic**. (Optional) The **default** option sets data rates 1, 2, 5.5, 6, 11, 12, and 24 to basic, and data rates 9, 18, 36, 48, and 54 to enabled. These data rate settings allow both 802.11b and 802.11g client devices to associate to the WMIC's 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:

```
bridge# configure terminal
bridge(config)# interface dot11radio 0
bridge(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
bridge(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 WMIC for 54 Mbps service only:

```
bridge# configure terminal
bridge(config)# interface dot11radio 0
bridge(config-if)# speed basic-54.0
bridge(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

Beginning in privileged EXEC mode, follow these steps to set the transmit power on your WMIC 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	**power local** {**1** | **5** | **10** | **20** | **30** | **50** | **100** | **maximum** }	Set the transmit power for the radio to one of the power levels allowed in your regulatory domain. All settings are in mW. The settings allowed in your regulatory domain might differ from the settings listed here. The maximum power level for the 4.9-GHz (US Only, Public Safety) radio is 40 mW. The 2.4-GHz (802.11b/g) radio transmits at up to 100 mW for the 1, 2, 5.5, and 11 Mbps data rates. However, for the 6, 9, 12, 18, 24, 36, 48, and 54 Mbps data rates, the maximum transmit power for the 802.11g radio is 30 mW.
Step 4	**power client** {**1** | **5** | **10** | **20** | **30** | **50** | **100** | **maximum** }	Set the maximum power level allowed on client devices that associate to the WMIC 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 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 power command to return the power setting to **maximum**, the default setting.

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 radio is least congested; at startup, the WMIC 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 to each bridge. The channel settings on your WMIC correspond to the frequencies available in your regulatory domain. See Appendix B, “Channels and Antenna Settings,” for the frequencies allowed in your domain.

IEEE 802.11g (2.4-GHz Band)

The radio operates on 11 channels from 2412-MHz to 2462-MHz. Each channel covers 5 MHz, and the bandwidth for the channels overlaps slightly. For best performance, use channels that are not adjacent (such as 2412 and 2417) for bridges that are close to each other.

Beginning in privileged EXEC mode, follow these steps to set the WMIC’s radio channel:

	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	**channel** *frequency* | **least-congested**	Set the default channel for the WMIC radio. To search for the least-congested channel on startup, enter **least-congested**. These are the available frequencies (in MHz) for the 2.4-GHz radio: • channel 1—**2412** (Americas, EMEA, Japan, and China) • channel 2—**2417** (Americas, EMEA, Japan, and China) • channel 3—**2422** (Americas, EMEA, Japan, Israel, and China) • channel 4—**2427** (Americas, EMEA, Japan, Israel, and China) • channel 5—**2432** (Americas, EMEA, Japan, Israel, and China) • channel 6—**2437** (Americas, EMEA, Japan, Israel, and China) • channel 7—**2442** (Americas, EMEA, Japan, Israel, and China) • channel 8—**2447** (Americas, EMEA, Japan, Israel, and China) • channel 9—**2452** (Americas, EMEA, Japan, Israel, and China) • channel 10—**2457** (Americas, EMEA, Japan, and China) • channel 11—**2462** (Americas, EMEA, Japan, and China) • channel 12—**2467** (EMEA and Japan) • channel 13—**2474** (EMEA and Japan) • channel 14—**2484** (Japan) **Note** The frequencies allowed in your regulatory domain might differ from the frequencies listed here.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

4.9-GHz Band

This band is available only in the USA. The radio operates on 16 channels, either 5-MHz wide or 10-MHz wide between 4940-MHz and 4990-MHz for the public safety community. To reduce the interference between two consecutive intersections, use two different channels in line-of-sight, cascaded deployments.

The throughput is a minimum of 4 Mbps half-duplex at a range of one mile line-of-sight for a 5-MHz-wide channel, and 8 Mbps half-duplex at on mile line-of-sight range for a 10-MHz-wide channel.

Table 4-1 Radio Frequency Data Rates

Data Rate (Mbps)	Modulation on sub-carriers based on OFDM	RMS Transmit Power (dBm)	Receiver Sensitivity (dBm)	Signal-to-noise Ratio (dB)
10 MHz Channelization				
3	BPSK	19	-94	4

Table 4-1 Radio Frequency Data Rates

4.5	BPSK	19	-93	4
6	QPSK	19	-92	6
9	QPSK	19	-91	6
12	16-QAM	19	-87	11
18	16-QAM	18	-84	11
24	64-QAM	16	-78	20
27	64-QAM	15	-75	20
5 MHz Channelization				
1.5	BPSK	19	-97	4
2.25	BPSK	19	-96	4
3	QPSK	19	-95	6
4.5	QPSK	19	-94	6
6	16-QAM	19	-90	11
9	16-QAM	18	-87	11
12	64-QAM	16	-81	20
13.5	64-QAM	15	-78	20

spacing channel User Interface Command

Use the **spacing** privileged **EXEC** command to define allowable channels and center frequencies for the 4.9-GHz WMIC. Use **no** form of this command to reset the channels and center frequencies to defaults. Released in 12.3(JK).

spacing <*baseband_no*> [**channel** {*centerFrequency* | *channel_number* | *least-congested*}]

Note The **channel** command is not available when this command is entered in the configuration.

Syntax Description

baseband_no	Specifies the channel spacing in megahertz on the desired channel band. The frequency is either 5-MHz wide or 10-MHz wide.
centerFrequency	Specifies the center frequency in megahertz of the desired channel band. Supported frequencies are listed in Table 4-2.
channel_number	Supported channel number. Supported channels are listed in Table 4-2.
least-congested	Automatically scan for the best frequency.

Defaults

Table 4-2 Channels, Center Frequencies, and Channel Widths

Channel	Center Frequency	Channel Width
1	4940.5	not supported
2	4941.5	not supported
3	4942.5	5-MHz
4	4943.5	not supported
5	4944.5	not supported
6	4947.5	5-MHz
7	4952.5	5-MHz or 10-MHz
8	4957.5	5-MHz
9	4962.5	5-MHz or 10-MHz
10	4967.5	5-MHz
11	4972.5	5-MHz or10-MHz
12	4977.5	5-MHz
13	4982.5	5-MHz or 10-MHz
14	4985.5	not supported
15	4986.5	5-MHz
16	4987.5	not supported
17	4988.5	not supported
18	4989.5	not supported

Command Modes

Configuration interface

Examples

This example shows how to set the channel spacing to 5-MHz spacing and channel number to 13 on a root device.

```
WMIC(config-if)# spacing 5 channel 13
```

This example shows how to set the channel spacing to 10-MHz spacing and center frequency to 4982.5-MHz spacing on a root device. (Note that the command requires that the entry be 4982, as opposed to 4982.5.)

```
WMIC(config-if)# spacing 10 channel 4982
```

This example shows how to set the channel spacing 5-MHz spacing on a non-root device.

```
WMIC(config-if)# spacing 5
```

Related Commands

Command	Description
show controllers dot11radio 0	Display the radio controller information and status.

Enabling and Disabling World Mode (2.4-GHz Only)

You can configure the WMIC to support 802.11d world mode or Cisco legacy world mode. When you enable world mode, the WMIC 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 WMIC is using 802.11d or Cisco legacy world mode and automatically use world mode that matches the mode used by the WMIC. World mode is disabled by default.

Beginning in privileged EXEC mode, follow these steps to enable world mode:

	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	**world-mode** **dot11d country_code** *code* { **both** | **indoor** | **outdoor** } | **legacy**	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 WMIC. • 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 (2.4-GHz Only)

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 Wireless LAN Client Adapters support short preambles. Early models of Cisco Aironet Wireless LAN Adapters (PC4800 and PC4800A) require long preambles.
- Long—A long preamble ensures compatibility between the WMIC and all early models of Cisco Wireless LAN Adapters. If these client devices do not associate to your WMIC, 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 WMIC uses to receive and transmit data. There are three options for both the receive and the transmit antenna:

- Diversity—This default setting tells the WMIC to use the antenna that receives the best signal.
- Right—If you install a high-gain antenna on the right connector and no antenna on the left connector, you should use this setting for both receive and transmit.
- Left—If you install a high-gain antenna on the left connector and no antenna on the right connector, use this setting for both receive and transmit.

Note The **antenna** commands are not available for 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.
Step 3	**antenna receive** {**diversity** | **left** | **right**}	Set the receive antenna to diversity, left, or right. **Note** For best performance, leave the receive antenna setting at the default setting, **diversity**.
Step 4	**antenna transmit** {**diversity** | **left** | **right**}	Set the transmit antenna to diversity, left, or right. **Note** For best performance, leave the transmit antenna setting at the default setting, **diversity**.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Note The **Antenna Gain (dB)** setting is disabled on the WMIC.

Configuring the Ethernet Encapsulation Transformation Method

When the WMIC receives data packets that are not 802.3 packets, the WMIC 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 wireless products. This is the default setting.
- RFC1042—Use this setting to ensure interoperability with non-Cisco 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 RFC1042 | dot1h**	Set the encapsulation transformation method to 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 bridge links, adjust the CW-min and CW-max contention window settings to to a value based on the number of non-root bridges associated to each root bridge. Refer to the "CW-min and CW-max Settings for Point-to-Point and Point-to-Multipoint Bridge Links" section on page 11-8 for instructions on adjusting these settings.

Enabling and Disabling Concatenation (2.4-GHz Only)

Use the **concatenation** command to enable packet concatenation on the WMIC radio. Using concatenation, the WMIC 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** *bytes*	(Optional) *Bytes* 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

Use the **distance** command to specify the distance from a root bridge to its clients (non-root bridges and/or workgroup bridges). The distance setting adjusts the time out values to account for the time required for radio signals for radio signals to travel from a root bridge to its clients (non-root bridges and/or workgroup bridges). If more than one non-root bridge (or workgroup bridge) communicates with the root bridge, enter the distance from the root bridge to the non-root bridge (or work-group bridge) that is farthest away. Enter a value from 0 to 99 km for a 2.4-GHz WMIC or 0 to 3 km for a 4.9-GHz WMIC. You do not need to adjust this setting on non-root 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 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** *kilometers*	Enter a distance setting from 0 to 99 km for a 2.4-GHz WMIC or 0 to 3 km for a 4.9-GHz WMIC.
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 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 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 4-16 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/bcfpart1/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** *group* **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** *interface-id*	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** *interface-id* **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

Configuring the Beacon Period

The beacon period is the amount of time between beacons in kilomicroseconds. One Kusec equals 1,024 microseconds. The default beacon period is 100. 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** *value*	Set the beacon period. Enter a value between 20 and 4000 Kusecs.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**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 WMIC 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 WMIC, or in areas where the clients are far apart and can detect only the WMIC and not each other. You can enter a setting ranging from 0 to 2339 bytes.

Note When concatenation is enabled for a 2.4-GHz WMIC, the RTS and fragment thresholds are set to 4000. Changing them to a lower value might degrade device performance. The 4.9-GHz WMIC does not support concatenation.

Maximum RTS Retries is the maximum number of times the WMIC 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 value for RTS retries 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** *value*	Set the RTS threshold. Enter an RTS threshold from 0 to 2339 for a 2.4-GHz WMIC or 0 to 4000 for a 4.9-GHz WMIC.
Step 4	**rts retries** *value*	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 WMIC 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** *value*	Set the maximum data retries. Enter a setting from 1 to 128.
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 for the 2.4-GHz WMIC, the RTS and fragment thresholds are set to 4000. Changing them to a lower value may degrade performance. The 4.9-GHz WMIC does not support concatenation.

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** *value*	Set the fragmentation threshold. Enter a setting from 256 to 4000 bytes.
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 bridge or workgroup bridge tries to associate with a parent access point. The command defines how long the 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** *seconds*	The **seconds** value specifies the amount of time in seconds the non-root 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.

Caution This command should not be used to configure a workgroup bridge or a non-root bridge a mobile application, as this feature adversely effects roaming time. If the same devices are used for stationary applications the **parent** command can be configured.

Beginning in privileged EXEC mode, follow these steps to configure up to four parent MAC addresses:

	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 the channels. During the carrier busy test, the WMIC 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:

dot 11 dot11Radio *interface-number* **carrier busy**

where, *interface-number* is the dot11radio interface.

Use the **show dot11 carrier busy** command to re-display the carrier busy test results.

Configuring SSIDs

This chapter describes how to configure a service set identifier (SSID) on the WMIC. This chapter contains these sections:

- Understanding SSIDs, page 5-2
- Configuring the SSID, page 5-2

Understanding SSIDs

The SSID is a unique identifier that wireless networking devices use to establish and maintain wireless connectivity. Multiple bridges on a network or sub-network can use the same SSID. SSIDs are case sensitive and can contain up to 32 alphanumeric characters. Do not include spaces in your SSID. The WMIC supports multiple SSIDs.

When you configure an SSID you assign these configuration settings to the SSID:

- VLAN
- RADIUS accounting for traffic using the SSID
- Authentication method

Note For detailed information on client authentication types, see Chapter 8, "Configuring Authentication Types."

If you want the WMIC to allow associations from bridges that do not specify an SSID in their configurations, you can include the SSID in the beacon. The default SSID, *autoinstall*, is included in the beacon. However, to keep your network secure, you should remove the SSID from the beacon.

You can assign an authentication username and password to the SSID to allow the WMIC to authenticate to your network using LEAP authentication.

If your network uses VLANs, you should assign the WMIC SSID to your network's native VLAN.

Configuring the SSID

These sections contain configuration information for the SSID:

- Default SSID Configuration, page 5-2
- Creating an SSID, page 5-3

Default SSID Configuration

Table 5-1 shows the default SSID configuration:

Table 5-1 Default SSID Configuration

Feature	Default Setting
SSID	autoinstall
Guest Mode SSID	autoinstall (The WMIC broadcasts this SSID in its beacon and allows bridges with no SSID to associate.)

Creating an SSID

Beginning in privileged EXEC mode, follow these steps to create 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*	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** You can include spaces in an SSID, but be careful not to add spaces to an SSID accidentally, especially at the end of an SSID.
Step 4	**authentication client** **username** *username* **password** *password*	(Optional) Set an authentication username and password that the WMIC uses to authenticate to the network.
Step 5	**accounting** *list-name*	(Optional) Enable RADIUS accounting for this SSID. For *list-name*, 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 6	**vlan** *vlan-id*	(Optional) Assign the SSID to a VLAN on your network. On your WMIC, you should assign the SSID to the native VLAN.
Step 7	**infrastructure-ssid**	Designate the SSID as the infrastructure SSID. It is used to instruct a non-root bridge or workgroup bridge radio to associate with this SSID.
Step 8	**end**	Return to privileged EXEC mode.
Step 9	**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 the SSID. See Chapter 8, "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
- Assign the SSID to the native VLAN
- Designate the SSID as the infrastructure SSID

```
bridge# configure terminal
bridge(config)# interface dot11radio 0
bridge(config-if)# ssid bridgeman
bridge(config-ssid)# accounting accounting-method-list
bridge(config-ssid)# vlan 1
bridge(config-ssid)# infrastructure-ssid
bridge(config-ssid)# end
```

CHAPTER 6

Configuring Spanning Tree Protocol

This chapter descibes how to configure Spanning Tree Protocol (STP) on your WMIC. This chapter contains these sections:

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

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 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 device that provides the most efficient path to the device 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 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 bridge supports both per-VLAN spanning tree (PVST) and a single 802.1q spanning tree without VLANs. The bridge cannot run 802.1s MST or 802.1d Common Spanning Tree, which maps multiple VLANs into a one-instance spanning tree.

The bridge maintains a separate spanning-tree instance for each active VLAN configured on it. A bridge ID, consisting of the bridge priority and the MAC address, is associated with each instance. For each VLAN, the bridge with the lowest bridge ID becomes the spanning-tree root for that VLAN.

Bridge Interoperability

Cisco 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 bridge acts as an access point and disallows association of non-root bridge.
- The 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 bridge STP feature is enabled and VLANs are not configured.

Note When the Cisco 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.

Bridge Protocol Data Units

The stable, active spanning-tree topology of your network is determined by these elements:

- The unique bridge ID (wireless bridge priority and MAC address) associated with each VLAN on each wireless 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 bridges in a network are powered up, each bridge functions as the STP root. The 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 bridge ID of the wireless bridge that the sending bridge identifies as the spanning-tree root
- The spanning-tree path cost to the root
- The bridge ID of the sending bridge
- Message age
- The identifier of the sending interface
- Values for the hello, forward delay, and max-age protocol timers

When a bridge receives a configuration BPDU that contains *superior* information (lower 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 bridge, the bridge also forwards it with an updated message to all attached LANs for which it is the designated bridge.

If a bridge receives a configuration BPDU that contains *inferior* information to that currently stored for that port, it discards the BPDU. If the bridge is a designated 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 bridge is elected as the spanning-tree root.
- A root port is selected for each bridge (except the spanning-tree root). This port provides the best path (lowest cost) when the bridge forwards packets to the spanning-tree root.
- The shortest distance to the spanning-tree root is calculated for each bridge based on the path cost.
- A designated bridge for each LAN segment is selected. The designated bridge incurs the lowest path cost when forwarding packets from that LAN to the spanning-tree root. The port through which the designated 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 bridges in the Layer 2 network participating in STP gather information about other 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 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 bridge with the highest bridge priority (the lowest numerical priority value) is elected as the spanning-tree root. If all bridges are configured with the default priority (32768), the bridge with the lowest MAC address in the VLAN becomes the spanning-tree root. The bridge priority value occupies the most significant bits of the bridge ID.

When you change the bridge priority value, you change the probability that the bridge will be elected as the root 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 bridge and its ports, including bridge and MAC addresses, 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 6-1 describes the timers that affect the entire spanning-tree performance.

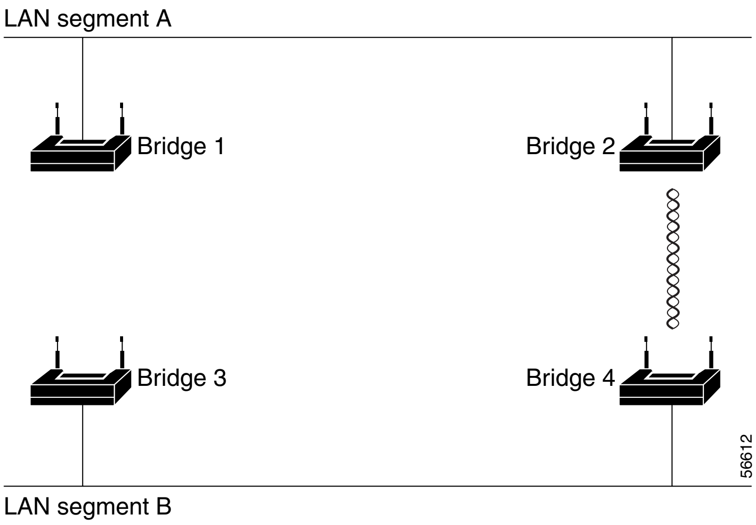
Table 6-1 Spanning-Tree Timers

Variable	Description
Hello timer	Determines how often the bridge broadcasts hello messages to other 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 bridge stores protocol information received on an interface.

Creating the Spanning-Tree Topology

In Figure 6-1, bridge 4 is elected as the spanning-tree root because the priority of all the 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 6-1 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 bridge using spanning tree exists in one of these states:

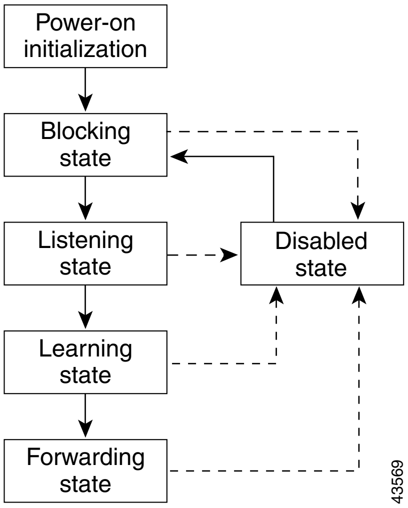
- Blocking—The interface does not participate in frame forwarding.
- Listening—The first transitional state after the blocking state when the spanning tree determines that the interface should participate in frame forwarding.
- Learning—The interface prepares to participate in frame forwarding.
- Forwarding—The 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 6-2 illustrates how an interface moves through the states.

Figure 6-2 Spanning-Tree Interface States



When you enable STP on the 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 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 bridge's Ethernet and radio ports. A bridge initially functions as the spanning-tree root until it exchanges BPDUs with other bridges. This exchange establishes which bridge in the network is the spanning-tree root. If there is only one 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 port is blocked, some broadcast or multicast packets can reach a forwarding port on the 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 WMIC:

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 6-9
- Configuring STP Settings, page 6-9
- STP Configuration Examples, page 6-10

Default STP Configuration

STP is disabled by default. Table 6-2 lists the default STP settings when you enable STP.

Table 6-2 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 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 WMIC:

	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.

	Command	Purpose
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.
Step 7	**bridge** *number* **priority** *priority*	(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 bridges with and without VLANs:

- Root Bridge Without VLANs, page 6-10
- Non-Root Bridge Without VLANs, page 6-11
- Root Bridge with VLANs, page 6-12
- Non-Root Bridge with VLANs, page 6-13

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 6-3:

*Table 6-3 Commands for Displaying Spanning-Tree Status*bridge

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 device.
show spanning-tree bridge	Displays status and configuration of this bridge.
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 *interface-id*	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 IOS Command Reference for Cisco Access Points and Bridges*.

Configuring WEP and WEP Features

This chapter describes how to configure Wired Equivalent Privacy (WEP), Message Integrity Check (MIC), and Temporal Key Integrity Protocol (TKIP). This chapter contains these sections:

- Understanding WEP, page 7-2
- Configuring Cipher Suites and WEP, page 7-3

Understanding WEP

Just as anyone within range of a radio station can tune to the station's frequency and listen to the signal, any wireless networking device within range of a bridge can receive the 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 radio communication between bridges to keep the communication private. Communicating bridges use the same WEP key to encrypt and unencrypt radio signals. WEP keys encrypt both unicast and multicast messages. Unicast messages are addressed to just one device on the network. Multicast messages are addressed to multiple devices on the network.

Extensible Authentication Protocol (EAP) authentication provides dynamic WEP keys to wireless devices. 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 8, "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:

- 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)—The Cisco WEP key permutation technique based on an early algorithm presented by the IEEE 802.11i security task group. (ckip and ckip-cmic are supported only on the 2.4-GHz (802.11b/g) WMIC.)
- CMIC (Cisco Message Integrity Check)—Like TKIP, the Cisco message integrity check mechanism is designed to detect forgery attacks.

Note If VLANs are enabled on your bridges, WEP, MIC, and TKIP are supported only on the native VLAN.

Configuring Cipher Suites and WEP

These sections describe how to configure cipher suites, WEP and additional WEP features such as MIC and TKIP:

- Creating WEP Keys, page 7-3
- Enabling Cipher Suites and WEP, page 7-5

WEP, TKIP, and MIC are disabled by default.

Creating 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.
Step 3	**encryption** [**vlan** *vlan-id*] **key** *1-4* **size** { **40** | **128** } *encryption-key* [**transmit-key**]	Create a WEP key and set up its properties. • (Optional) Select the VLAN for which you want to create a key. WEP, MIC, and TKIP are supported only on the native VLAN. • Name the key slot in which this WEP key resides. You can assign up to 4 WEP keys for each VLAN, but key slot 4 is reserved for the session key. • 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) Set this key as the transmit key. The key in slot 2 is the transmit key by default. If you enable WEP with MIC, use the same WEP key as the transmit key in the same key slot on both root and non-root bridges.
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 2 for VLAN 1 and sets the key as the transmit key:

```
bridge# configure terminal
bridge(config)# configure interface dot11radio 0
bridge(config-if)# encryption vlan 1 key 2 size 128 12345678901234567890123456
transmit-key
bridge(config-if)# end
```

WEP Key Restrictions

Table 7-1 lists WEP key restrictions based on your security configuration.

Table 7-1 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
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	Root and non-root bridges must use the same WEP key as the transmit key, and the key must be in the same key slot on both root and non-root bridges

Example WEP Key Setup

Table 7-2 shows an example WEP key setup that would work for the root bridge and an associated non-root bridge:

Table 7-2 WEP Key Setup Example

Key Slot	Root Bridge		Associated Non-Root Bridge	
	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 root bridge’s WEP key 1 is selected as the transmit key, WEP key 1 on the non-root bridge must have the same contents. WEP key 4 on the non-root bridge is set, but because it is not selected as the transmit key, WEP key 4 on the root 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 root bridge and any non-root bridges with which it communicates must use the same WEP key for transmitting data. For example, if the MIC-enabled root bridge uses the key in slot 1 as the transmit key, a non-root bridge associated to the root bridge must use the same key in its slot 1, and the key in the non-root bridge’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** *vlan-id*] **mode ciphers** {[**aes-ccm** | **ckip** | **cmic** | **ckip-cmic** | **tkip**]} {[**wep128** | **wep40**]}	Enable a cipher suite containing the WEP protection you need. Table 7-3 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** You can also use the **encryption mode wep** command to set up static WEP. However, you should use **encryption mode wep** only if none of the non-root bridges that associate to the root bridge are capable of key management. See the *Cisco IOS Command Reference for Cisco Access Points and Bridges* for a detailed description of the **encryption mode wep** command. **Note** When you configure **TKIP**-only cipher encryption (not **TKIP + WEP 128** or **TKIP + WEP 40**) on any radio interface or VLAN, the SSID on that radio or VLAN must be set to use WPA or CCKM key management. If you configure TKIP on a radio or VLAN but you do not configure key management on the SSID, non-root bridge authentication fails on the SSID. **Note** ckip and ckip-cmic are supported only on the 2.4-GHz (802.11b/g) WMIC.
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 1 that enables CKIP, CMIC, and 128-bit WEP.

```
bridge# configure terminal
bridge(config)# configure interface dot11radio 0
bridge(config-if)# encryption vlan 1 mode ciphers ckip-cmic wep128
bridge(config-if)# end
```

Matching Cipher Suites with WPA

If you configure your bridges to use WPA or CCKM authenticated key management, you must select a cipher suite compatible with the authenticated key management type. Table 7-3 lists the cipher suites that are compatible with WPA and CCKM.

Table 7-3 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 • encryption mode ciphers tkip wep128 • encryption mode ciphers tkip wep40
WPA	• encryption mode ciphers tkip • encryption mode ciphers tkip wep128 • encryption mode ciphers tkip wep40

Note When you configure **TKIP**-only cipher encryption (not **TKIP + WEP 128** or **TKIP + WEP 40**) on any radio interface or VLAN, the SSID on that radio or VLAN must be set to use WPA or CCKM key management. If you configure TKIP on a radio or VLAN but you do not configure key management on the SSID, non-root bridge authentication fails on the SSID.

For a complete description of WPA and CCKM and instructions for configuring authenticated key management, see the "Using WPA Key Management" section on page 8-5 and the "Using CCKM for Authenticated Bridges" section on page 8-5.

Configuring Authentication Types

This chapter describes how to configure authentication types on the WMIC. This chapter contains these sections:

Understanding Authentication Types

This section describes the authentication types that you can configure on the WMIC. The authentication types are tied to the SSID that you configure on the WMIC.

Before wireless devices can communicate, they must authenticate to each other using open or shared-key authentication. For maximum security, wireless devices should also authenticate to your network using EAP authentication, an authentication type that relies on an authentication server on your network.

The WMIC uses four authentication mechanisms or types and can use more than one at the same time. These sections explain each authentication type:

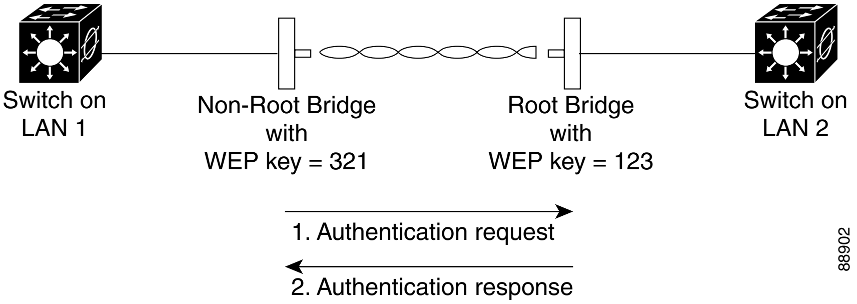
- Open Authentication to the WMIC, page 8-2
- Shared Key Authentication to the Bridge, page 8-2
- EAP Authentication to the Network, page 8-3

Open Authentication to the WMIC

Open authentication allows any wireless device to authenticate and then attempt to communicate with another wireless device. Using open authentication, a non-root bridge can authenticate to a root bridge. A bridge that is not using WEP does not attempt to authenticate with a bridge that is using WEP. Open authentication does not rely on a RADIUS server on your network.

Figure 8-1 shows the authentication sequence between a non-root bridge trying to authenticate and a root bridge using open authentication. In this example, the device's WEP key does not match the bridge's key, so it can authenticate but it cannot pass data.

Figure 8-1 Sequence for Open Authentication


Switch on LAN 1
Non-Root Bridge with WEP key = 321
Root Bridge with WEP key = 123
Switch on LAN 2
1. Authentication request
2. Authentication response
88902

Shared Key Authentication to the Bridge

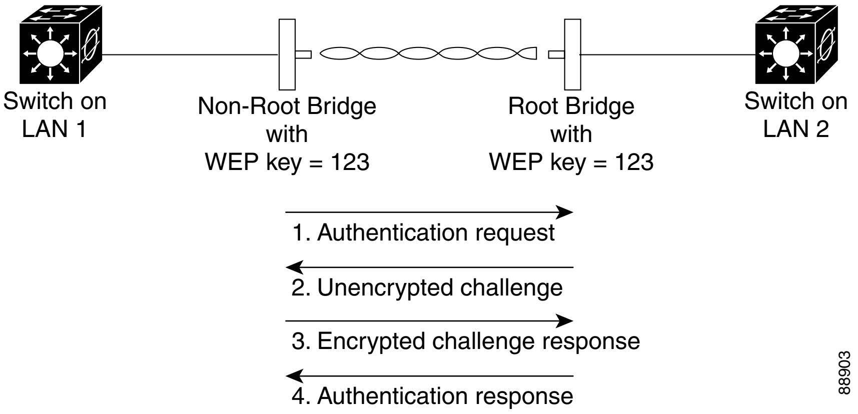
Cisco provides shared key authentication to comply with the IEEE 802.11b and IEEE 802.11g standards. However, because of shared key's security flaws, we recommend that you use another method of authentication, such as EAP, in environments where security is an issue.

During shared key authentication, the root bridge sends an unencrypted challenge text string to other bridges attempting to communicate with the root bridge. The bridge requesting authentication encrypts the challenge text and sends it back to the root bridge. If the challenge text is encrypted correctly, the root bridge allows the requesting device to authenticate.

Both the unencrypted challenge and the encrypted challenge can be monitored, however, which leaves the root bridge open to attack from an intruder who calculates the WEP key by comparing the unencrypted and encrypted text strings.

Figure 8-2 shows the authentication sequence between a device trying to authenticate and an bridge using shared key authentication. In this example the device's WEP key matches the bridge's key, so it can authenticate and communicate.

Figure 8-2 Sequence for Shared Key Authentication

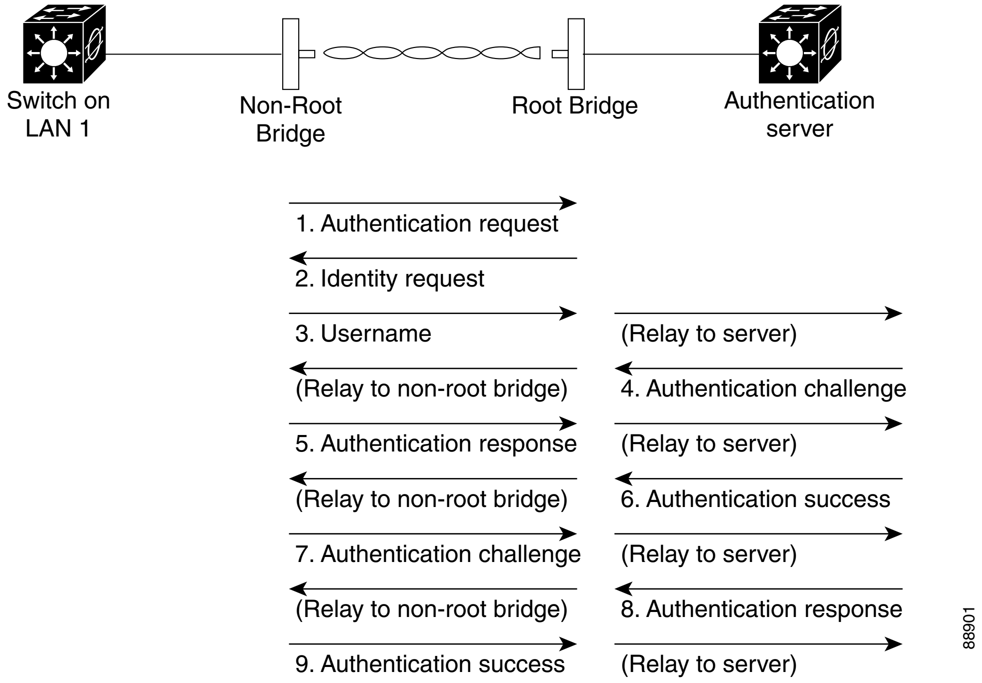

Switch on LAN 1
Non-Root Bridge with WEP key = 123
Root Bridge with WEP key = 123
Switch on LAN 2
1. Authentication request
2. Unencrypted challenge
3. Encrypted challenge response
4. Authentication response
88903

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 bridge helps another 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 bridge, which uses it for all unicast data signals that it sends to or receives from the non-root bridge. The root bridge also encrypts its broadcast WEP key (entered in the bridge's WEP key slot 1) with the non-root bridge's unicast key and sends it to the non-root bridge.

When you enable EAP on your bridges, authentication to the network occurs in the sequence shown in Figure 8-3:

Figure 8-3 Sequence for EAP Authentication


Switch on LAN 1
Non-Root Bridge
Root Bridge
Authentication server
1. Authentication request
2. Identity request
3. Username
(Relay to server)
(Relay to non-root bridge)
4. Authentication challenge
5. Authentication response
(Relay to server)
(Relay to non-root bridge)
6. Authentication success
7. Authentication challenge
(Relay to server)
(Relay to non-root bridge)
8. Authentication response
9. Authentication success
(Relay to server)
88901

In Steps 1 through 9 in Figure 8-3, a non-root bridge and a RADIUS server on the wired LAN use 802.1x and EAP to perform a mutual authentication through the root bridge. The RADIUS server sends an authentication challenge to the non-root bridge. The non-root 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 bridge. When the RADIUS server authenticates the non-root bridge, the process repeats in reverse, and the non-root bridge authenticates the RADIUS server.

When mutual authentication is complete, the RADIUS server and the non-root bridge determine a WEP key that is unique to the non-root bridge and provides the non-root 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 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 bridge. The root bridge encrypts its broadcast key with the session key and sends the encrypted broadcast key to the non-root bridge, which uses the session key to decrypt it. The non-root bridge and the root 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 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 8-6 for instructions on setting up EAP on the WMIC.

Note If you use EAP authentication, you can select open or shared key authentication, but you do not have to. EAP authentication controls authentication both to your bridge and to your network.

Using CCKM for Authenticated Bridges

Using Cisco Centralized Key Management (CCKM), authenticated non-root bridges can roam from one root bridge to another without any perceptible delay during reassociation. An access point or switch on your network provides Wireless Domain Services (WDS) and creates a cache of security credentials for CCKM-enabled bridges on the subnet. The WDS device's cache of credentials dramatically reduces the time required for reassociation when a CCKM-enabled non-root bridge roams to a new root bridge.

When a non-root bridge roams, the WDS device forwards the bridge's security credentials to the new root bridge, and the reassociation process is reduced to a two-packet exchange between the roaming bridge and the new root bridge. Roaming bridges 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 8-6 for instructions on enabling CCKM on your bridge.

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 the 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 bridges and the authentication server authenticate to each other using an EAP authentication method, and the non-root bridge and server generate a pairwise master key (PMK). Using WPA, the server generates the PMK dynamically and passes it to the root bridge. Using WPA-PSK, however, you configure a pre-shared key on both the non-root bridge and the root 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) might 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 bridge and the non-root 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 bridge is disassociated from the wireless LAN.

See the "Assigning Authentication Types to an SSID" section on page 8-6 for instructions on configuring WPA key management on your bridge.

Configuring Authentication Types

This section describes how to configure authentication types. You attach configuration types to the WMIC's SSID. See Chapter 5, "Configuring SSIDs," for details on setting up the WMIC SSID. This section contains these topics:

- Default Authentication Settings, page 8-6
- Assigning Authentication Types to an SSID, page 8-6
- Configuring Authentication Holdoffs, Timeouts, and Intervals, page 8-10

Default Authentication Settings

The default SSID on the WMIC is *autoinstall*. Table 8-1 shows the default authentication settings for the default SSID:

Table 8-1 Default Authentication Configuration

Feature	Default Setting
SSID	autoinstall
Guest Mode SSID	autoinstall (The WMIC broadcasts this SSID in its beacon and allows bridges with no SSID to associate.)
Authentication types assigned to tsunami	open

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** *ssid-string*	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** [**eap** *list-name*]	(Optional) Set the authentication type to open for this SSID. Open authentication allows any bridge to authenticate and then attempt to communicate with the WMIC. • (Optional) Set the SSID's authentication type to open with EAP authentication. The WMIC forces all other bridges to perform EAP authentication before they are allowed to join the network. For *list-name*, specify the authentication method list. **Note** A bridge configured for EAP authentication forces all bridges that associate to perform EAP authentication. Bridges that do not use EAP cannot communicate with the bridge.
Step 5	**authentication shared** [**eap** *list-name*]	(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. • (Optional) Set the SSID's authentication type to shared key with EAP authentication. For list-name, specify the authentication method list.

	Command	Purpose
Step 6	**authentication network-eap** *list-name*	(Optional) Set the authentication type for the SSID to use LEAP for authentication and key distribution. Cisco bridges only support LEAP, while other wireless clients may support other EAP methods such as EAP, PEAP, or TLS.
Step 7	**authentication key-management** {[**wpa**] [**cckm**]} [**optional**]	(Optional) Set the authentication type for the SSID to WPA, CCKM, or both. If you use the **optional** keyword, non-root bridges not configured for WPA or CCKM can use this SSID. If you do not use the **optional** keyword, only WPA or CCKM bridges are allowed to use the SSID. To enable CCKM for an SSID, you must also enable Network-EAP authentication. To enable WPA for an SSID, you must also enable Open authentication or Network-EAP or both. **Note** Only 802.11b and 802.11g radios support WPA and CCKM simultaneously. **Note** Before you can enable CCKM or WPA, you must set the encryption mode for the SSID's VLAN to one of the cipher suite options. To enable both CCKM and WPA, you must set the encryption mode to a cipher suite that includes TKIP. See the "Enabling Cipher Suites and WEP" section on page 7-5 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 8-9 for instructions on configuring a pre-shared key. **Note** To support CCKM, your root bridge must interact with the WDS device on your network. See the "Configuring the Root Bridge to Interact with the WDS Device" section on page 8-8 for instructions on configuring your root bridge to interact with your WDS device.
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 *bridgeman* to open with EAP authentication. Bridges using the SSID *bridgeman* attempt EAP authentication using a server named *adam*.

```
bridge# configure terminal
bridge(config)# configure interface dot11radio 0
bridge(config-if)# ssid bridgeman
bridge(config-ssid)# authentication open eap adam
bridge(config-ssid)# end
```

The configuration on non-root bridges associated to this bridge would also contain these commands:

```
bridge(config)# configure interface dot11radio 0
bridge(config-if)# ssid bridgeman
bridge(config-ssid)# authentication client username bridge7 password catch22
bridge(config-ssid)# authentication open eap adam
```

This example sets the authentication type for the SSID *bridget* to network EAP with a static WEP key. EAP-enabled bridges using the SSID *bridget* attempt EAP authentication using a server named *eve*, and bridges using static WEP rely on the static WEP key.

```
bridge#configure terminal
bridge#aaa new-model
bridge#aaa group server radius rad_eap
bridge#server 13.1.1.99 auth-port 1645 acct-port 1646
bridge#aaa authentication login eap_methods group rad_eap
bridge#aaa session-id common
bridge(config)#interface dot11radio 0
bridge(config-if)#encryption key 1 size 128bit 7  082CC74122FD8DA7E84856427E9D
transmit-key
bridge(config-if)#encryption mode wep mandatory
bridge(config-if)# ssid bridget
bridge(config-ssid)# authentication network-eap eap_methods
bridge(config-ssid)# authentication network-eap eve
bridge(config-ssid)# infrastructure-ssid
bridge(config-ssid)# radius-server host 13.1.1.99 auth-port 1645 acct-port 1646 key 7
141B1309
bridge(config-ssid)# radius-server authorization permit missing Service-Type
bridge(config-ssid)# end
```

The configuration on non-root bridges associated to this bridge would also contain these commands:

```
bridge(config)# configure interface dot11radio 0
bridge(config)# encryption key 1 size 128bit 7  06061D688B87F1A0C978330C1A84 transmit-key
bridge(config)# encryption mode wep mandatory
bridge(config-if)# ssid bridget
bridge(config-if)# authentication network-eap eap_methods
bridge(config-if)# authentication client username thomasd password 7 010012165E18155D
bridge(config-if)# infrastructure-ssid
```

Configuring the Root Bridge to Interact with the WDS Device

To support non-root bridges using CCKM, your root 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 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 Access Points*.

On your root bridge, enter this command in global configuration mode:

```
bridge(config)# wlccp ap username username password password
```

You must configure the same username and password pair when you set up the root bridge as a client on your authentication server.

Configuring Additional WPA Settings

Use two optional settings to configure a pre-shared key on the 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 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 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 root bridge distributes a group key to the authenticated non-root bridge. You can use these optional settings to configure the root bridge to change and distribute the group key based on association and disassociation of non-root bridges:

- Membership termination—the root bridge generates and distributes a new group key when any authenticated non-root bridge disassociates from the root bridge. This feature keeps the group key private for associated bridges.
- Capability change—the root bridge generates and distributes a dynamic group key when the last non-key management (static WEP) non-root bridge disassociates, and it distributes the statically configured WEP key when the first non-key management (static WEP) non-root bridge authenticates. In WPA migration mode, this feature significantly improves the security of key-management capable clients when there are no static-WEP bridges associated to the root 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.
Step 4	**wpa-psk** { **hex** | **ascii** } [**0** | **7**] *encryption-key*	Enter a pre-shared key for 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 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 bridges using WPA and static WEP, with group key update options:

```
bridge# configure terminal
bridge(config)# configure interface dot11radio 0
bridge(config-if)# ssid batman
bridge(config-ssid)# wpa-psk ascii batmobile65
bridge(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 bridges authenticating through your root bridge:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**dot11 holdoff-time** *seconds*	Enter the number of seconds a root 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** *seconds*	Enter the number of seconds the bridge should wait for a reply from a non-root bridge attempting to authenticate before the authentication fails. Enter a value from 1 to 65555 seconds.
Step 5	**dot1x reauth-period** *seconds* [**server**]	Enter the interval in seconds that the WMIC waits before forcing an authenticated non-root bridge to reauthenticate. • (Optional) Enter the **server** keyword to configure the 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 bridge before termination of the session or prompt. The server sends this attribute to the root bridge when a non-root 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.

Setting Up a Non-Root Bridge as a LEAP Client

You can set up a non-root bridge to authenticate to your network like other wireless client devices. After you provide a network username and password for the non-root bridge, it authenticates to your network using LEAP, Cisco's wireless authentication method, and receives and uses dynamic WEP keys.

Setting up a non-root bridge as a LEAP client requires three major steps:

1. Create an authentication username and password for the non-root bridge on your authentication server.
2. Configure LEAP authentication on the root bridge to which the non-root bridge associates.
3. Configure the non-root bridge to act as a LEAP client.

Beginning in Privileged Exec mode, follow these instructions to set up the non-root bridge 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.
Step 3	**ssid** *ssid-string*	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 client username** *username* **password** *password*	Configure the username and password that the non-root bridge uses when it performs LEAP authentication. This username and password must match the username and password that you set up for the non-root bridge on the authentication server.
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 sets a LEAP username and password for the SSID bridgeman:

```
bridge# configure terminal
bridge(config)# configure interface dot11radio 0
bridge(config-if)# ssid bridgeman
bridge(config-ssid)# authentication client username bugsy password run4yerlife
bridge(config-ssid)# end
```

Matching Authentication Types on Root and Non-Root Bridges

To use the authentication types described in this section, the root bridge authentication settings must match the settings on the non-root bridges that associate to the root bridge.

Table 8-2 lists the settings required for each authentication type on the root and non-root bridges.

Table 8-2 Client and Bridge Security Settings

Security Feature	Non-Root Bridge Setting	Root Bridge Setting
Static WEP with open authentication	Set up and enable WEP	Set up and enable WEP and enable Open Authentication
Static WEP with shared key authentication	Set up and enable WEP and enable Shared Key Authentication	Set up and enable WEP and enable Shared Key Authentication
LEAP authentication	Configure a LEAP username and password	Set up and enable WEP and enable network-EAP authentication

Table 8-2 Client and Bridge Security Settings (continued)

Security Feature	Non-Root Bridge Setting	Root Bridge Setting
CCKM key management	Set up and enable WEP and enable CCKM authentication	Set up and enable WEP and enable CCKM authentication, configure the root bridge to interact with your WDS device, and add the root bridge to your authentication server as a client device
WPA key management	Set up and enable WEP and enable WPA authentication	Set up and enable WEP and enable WPA authentication

LEAP Example Configurations

Workgroup Bridge

```
aaa new-model
!
aaa group server radius rad_eap
 server 172.16.8.151 auth-port 1645 acct-port 1646
!
aaa authentication login eap_methods group rad_eap
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption key 1 size 128bit 0 123456789012334567890123456 transmit-key
 encryption mode wep mandatory
 !
 ssid silicon_beach_hotspot
    authentication network-eap eap_methods
    authentication client username officer1 password 0 beach123
```

Access Point

```
aaa new-model
!
aaa group server radius rad_eap
 server 172.16.8.151 auth-port 1645 acct-port 1646
!
aaa authentication login eap_methods group rad_eap
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
encryption key 1 size 128bit 7 A56C276D6B9560D2F4267B256926 transmit-key
 encryption mode wep mandatory
 !
 ssid silicon_beach_wep
    authentication network-eap eap_methods
```

CHAPTER 9

Configuring WDS, Fast Secure Roaming, and Radio Management

This chapter describes how to configure access points for wireless domain services (WDS), fast, secure roaming of client devices, and radio management. This chapter contains these sections:

- Understanding WDS, page 9-2
- Understanding Fast Secure Roaming, page 9-3
- Understanding Radio Management, page 9-4
- Configuring WDS and Fast Secure Roaming, page 9-5
- Using Debug Messages, page 9-13

Understanding WDS

The following sections describe WDS even though the WMIC cannot be configured as a WDS server even when it is configured as an access point. However, when configured as an access point, the WMIC can use a WDS server and can act as a WDS authenticator (client).

When you configure an access point to provide WDS, other access points (such as your WMIC if it is configured as an access point) on your wireless LAN use the WDS access point to provide fast, secure roaming for client devices and to participate in radio management.

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 access point. The WDS access point aggregates the information and forwards it to a wireless LAN solution engine (WLSE) device on your network.

Role of the WDS Access Point

The WDS access point performs several tasks on your wireless LAN:

- Advertises its WDS capability and participates in electing the best WDS access point for your wireless LAN. When you configure your wireless LAN for WDS, you set up one access point as the main WDS access point candidate and one or more additional access points as backup WDS access point candidates.
- 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.
- Registers all client devices in the subnet, establishes session keys for them, and caches their security credentials. When a client roams to another access point, the WDS access point forwards the client's security credentials to the new access point.

Role of Access Points Using the WDS Access Point

The access points on your wireless LAN interact with the WDS access point in these activities:

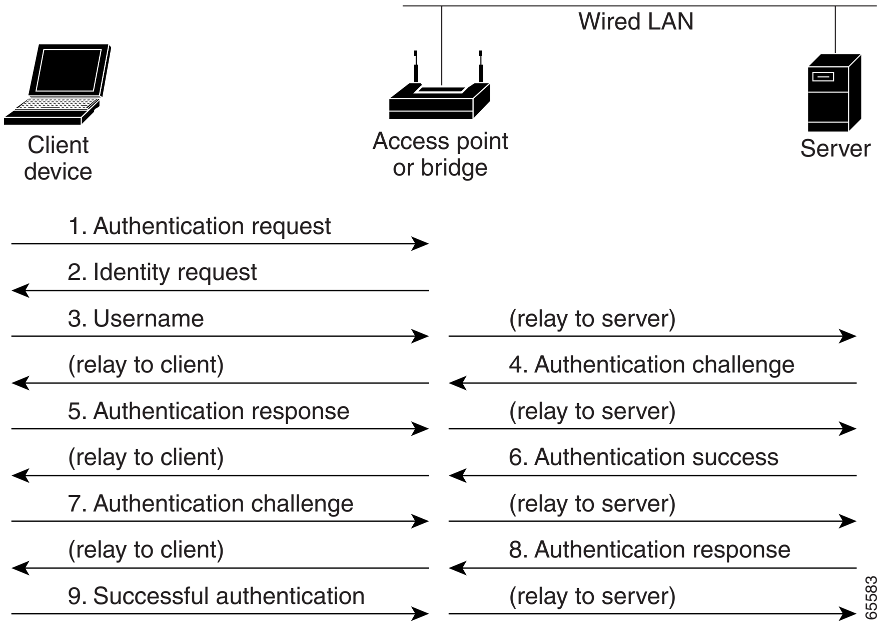
- Discover and track the current WDS access point and relay WDS advertisements to the wireless LAN.
- Authenticate with the WDS access point and establish a secure communication channel to the WDS access point.
- Register associated client devices with the WDS access point.
- Report radio data to the WDS access point.

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.

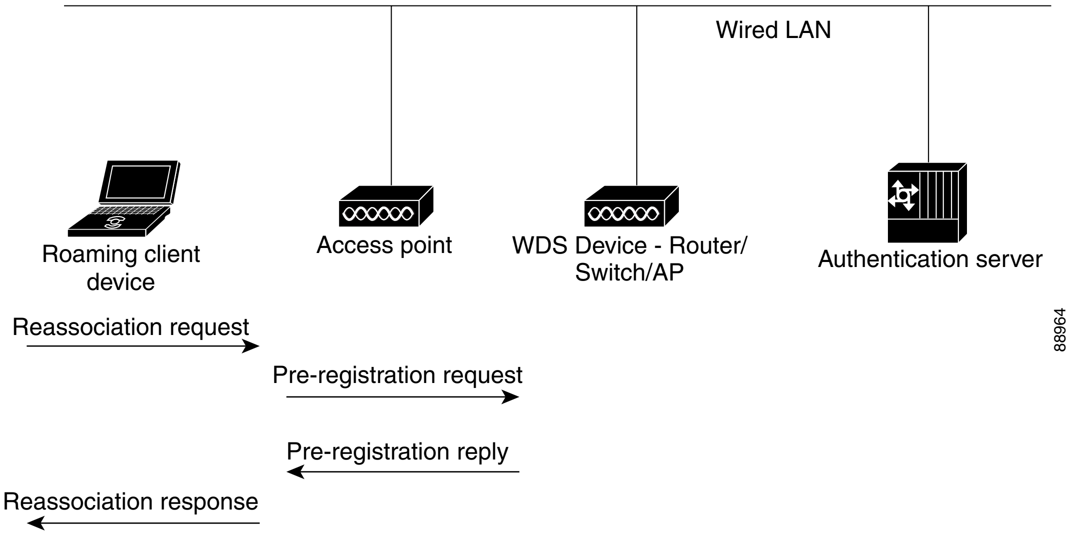
During normal operation, LEAP-enabled client devices mutually authenticate with a new access point by performing a complete LEAP authentication, including communication with the main RADIUS server, as in Figure 9-1.

Figure 9-1 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 server. Using Cisco Centralized Key Management (CCKM), an access point 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 9-2 shows client authentication using CCKM.

Figure 9-2 Client Reassociation Using CCKM and a WDS Access Point



The WDS access point 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 access point. The WDS access point 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.

Understanding Radio Management

Access points participating in radio management scan the radio environment and send reports to the WDS access point on such radio information as potential rogue access points, associated clients, client signal strengths, and the radio signals from other access points. The WDS access point forwards the aggregated radio data to the WLSE device on your network. Access points 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 "" section on page 9-13 for instructions on configuring radio management.

Configuring WDS and Fast Secure Roaming

This section describes how to configure WDS and fast, secure roaming on your wireless LAN. This section contains these sections:

Guidelines for WDS

You should be aware of these WDS guidelines:

- You cannot configure your WMIC as a WDS access point. However, when you configure your WMIC as an access point, you can also configure it to use the WDS access point.
- Repeater access points do not support WDS.

Requirements for WDS and Fast Secure Roaming

The wireless LAN on which your WMIC resides must meet these requirements:

- Central wireless domain services (WDS) server serving a zone (see the Configuring WDS, Fast Secure Roaming, and Radio Management chapter for more information)
- Root devices configured to communicate with Central WDS server for the zone
- Root devices on subnet / zone boundaries configured to allow unauthenticated traffic only to home agent
- MoIP in foreign agent mode

Configuring the WMIC to use the WDS Access Point

Your WMIC must be configured as an access point before you can configure it to use WDS. Configure the WMIC to authenticate through the WDS access point and participate in CCKM.

```
AP# configure terminal
AP(config)# wlccp ap username APWestWing password 7 wes7win8
AP(config)# end
```

In this example, the WMIC is enabled to interact with the WDS access point, 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.

Also, to configure an access point to use a WDS access point, the access point must be configured for an encryption cipher and authentication methods. For example:

```
encryption mode ciphers ckip-cmic
 !
 ssid kin_leap
    authentication network-eap eap_methods
    authentication key-management cckm
```

Refer to the "Configuring Authentication Types" chapter for more information.

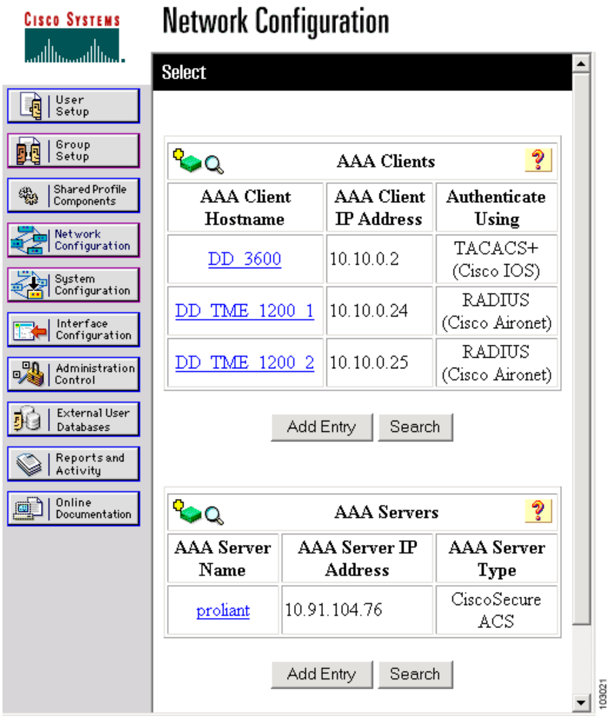
Configuring the Authentication Server to Support Fast Secure Roaming

The WDS access point and all access points participating in CCKM 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 access point.

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 access point. Figure 9-3 shows the Network Configuration page.

Figure 9-3 Network Configuration Page



AAA Clients

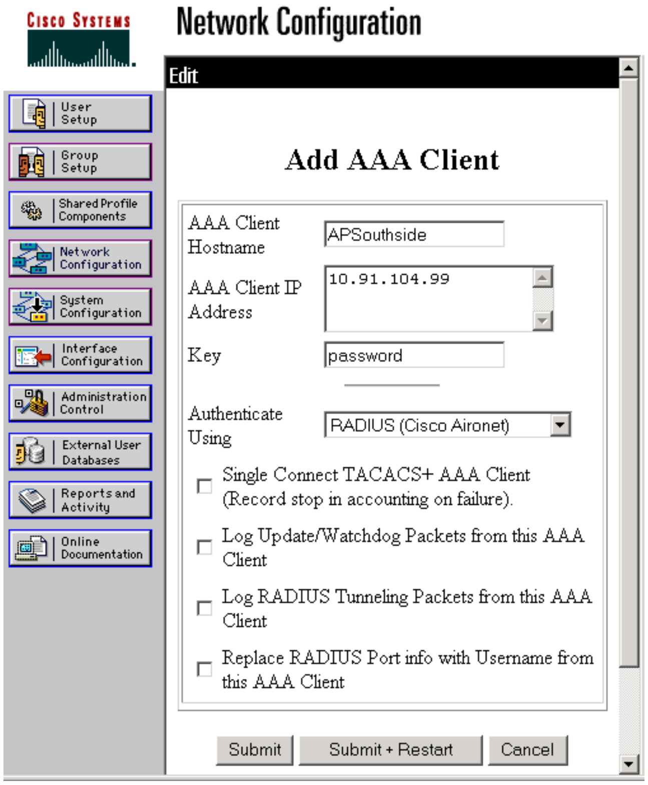
AAA Client Hostname	AAA Client IP Address	Authenticate Using
DD_3600	10.10.0.2	TACACS+ (Cisco IOS)
DD_TME_1200_1	10.10.0.24	RADIUS (Cisco Aironet)
DD_TME_1200_2	10.10.0.25	RADIUS (Cisco Aironet)

AAA Servers

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 9-4 shows the Add AAA Client page.

Figure 9-4 Add AAA Client Page



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

Step 3 In the AAA Client Hostname field, enter the name of the WDS access point.

Step 4 In the AAA Client IP Address field, enter the IP address of the WDS access point.

Step 5 In the Key field, enter exactly the same password that is configured on the WDS access point.

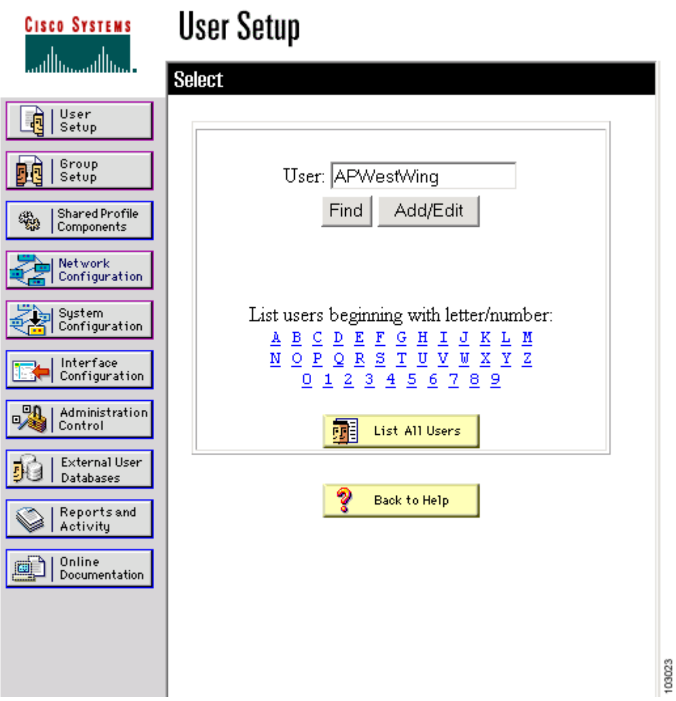
Step 6 From the Authenticate Using drop-down menu, select **RADIUS**.

Step 7 Click **Submit**.

Step 8 Repeat Step 2 through Step 7 for each WDS access point 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 access point. Figure 9-5 shows the User Setup page.

Figure 9-5 User Setup Page



User: APWestWing

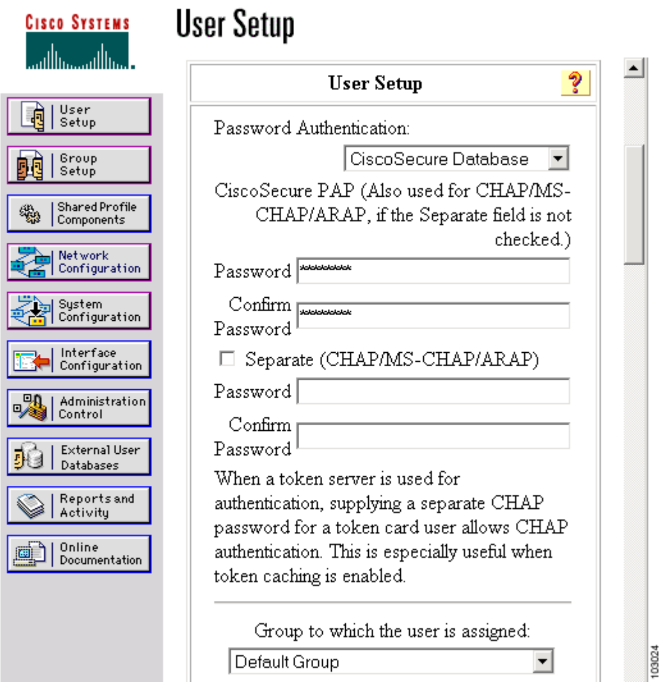
List users beginning with letter/number:

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 9-6 shows the User Setup box.

Figure 9-6 ACS User Setup Box



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.

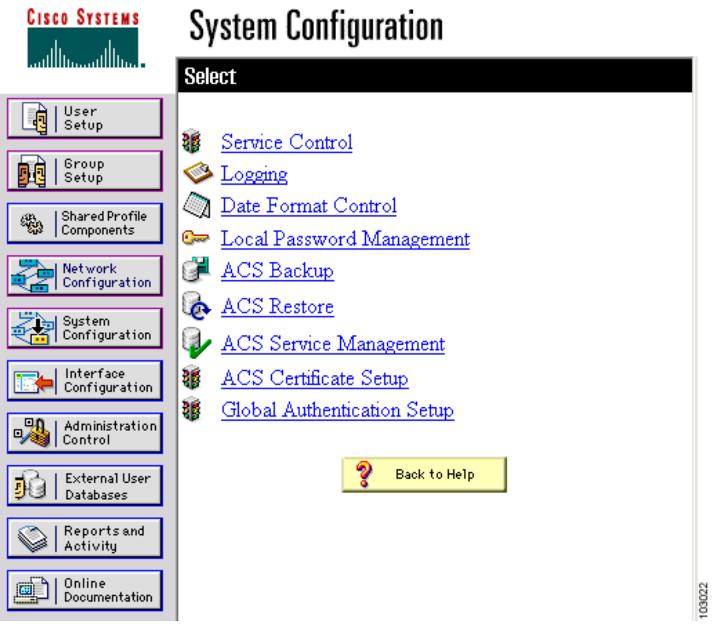
Step 14 In the Password and Confirm Password fields, enter exactly the same password that you entered on the access point on the Wireless Services AP page.

Step 15 Click **Submit**.

Step 16 Repeat Step 10 through Step 15 for each access point that uses the WDS access point.

Step 17 Browse to the System Configuration page, click **Service Control**, and restart ACS to apply your entries. Figure 9-7 shows the System Configuration page.

Figure 9-7 ACS System Configuration Page



CLI Commands to Enable the WDS Server

The following CLI commands are required to enable the WDS server. The **no** form of the commands disables the WDS server. The same configuration applies for Central WDS server and per subnet WDS server.

```
[no] wlccp wds priority <1-255> interface BVI1
[no] wlccp authentication-server infrastructure <method_infra>
where <method_infra> is <authentication server list name>
[no] wlccp authentication-server client [any | eap | leap | mac] <method_client>
where <method_ client > is <authentication server list name>
[no] aaa group server radius infra
    [no] server <IP address of RADIUS server> auth-port <Port number> acct-port <Port
    number>
[no] aaa group server radius client
    [no] server <IP address of RADIUS server> auth-port <Port number> acct-port <Port
    number>
[no] aaa authentication login <method_infra> group infra
where <method_infra> is <named authentication list>
[no] aaa authentication login <method_client> group client
```

```
where <method_ client > is <named authentication list>
```

CLI Commands to Enable the Root Device

The following CLI commands are required to enable the root device to communicate with the Central WDS server. The **no** form disables the WDS server. This configuration also allows the Root device to authenticate with per subnet WDS server if the Central WDS server fails.

```
[no] wlccp ap wds ip address <IP address of the WDS>
[no] wlccp ap username <WLCCP user name> password 0 <The UNENCRYPTED (cleartext) LEAP
password>
[no] interface Dot11Radio0
    [no] encryption mode ciphers [aes-ccm | tkip | wep128 | wep40]
    [no] ssid <radio Service Set ID>
[no] authentication network-eap <eap_methods>
               where <eap_methods> is <leap list name>
[no] authentication key-management cckm
[no] aaa group server radius rad_eap
    [no] server <IP address of RADIUS server> auth-port <Port number> acct-port <Port
    number>
[no] aaa authentication login <eap_methods> group rad_eap
where <eap_methods> is <named authentication list>
```

The **authentication network-eap <eap_methods>** command allows traffic to and from the client while it is being authenticated by the root device. This command should be entered on all the root devices located in zone boundaries and on all the clients.

```
authentication network-eap <eap_methods> <non-blocking>
```

where **<non-blocking>** allows a client to send or receive traffic while the root device is authenticating the client.

To enable blocking of client traffic during authentication, enter the command without the **non-blocking** keyword.

```
authentication network-eap <eap_methods>
```

Refer to http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ibm_r1/ib1_a1g.pdf for details on configuring access control lists on an access point to allow clients to send traffic to a home agent only.

Refer to http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/iprmb_r/ip4bookg.pdf for details on Mobile IP configuration commands.

Refer to http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/gtfamoip.htm for details on the *foreign agent local routing* feature and its configuration details.

dot11 interface speed Command

The **dot11 interface** *speed* command supports only 4.9-GHz data rates. The configured spacing has precedence over the default spacing. For example, if 5-MHz spacing is configured, only data rates corresponding to 5-MHz spacing can be specified in the *speed* command. If an incorrect data rate is specified for the currently configured spacing, an error message displays, "Incorrect data rate for currently configured spacing."

```
[no] interface Dot11Radio0
[no] speed <data rate>
```

where *data rate* can be one of the following:

Data Rate	Description	Spacing
1.5	Allow 1.5 Mbps	5-MHz
2.25	Allow 2.25 Mbps	5-MHz
3.0	Allow 3.0 Mbps	5-MHz and 10-MHz
4.5	Allow 4.5 Mbps	5-MHz and 10-MHz
6.0	Allow 6.0 Mbps	5-MHz and 10-MHz
9.0	Allow 9.0 Mbps	5-MHz and 10-MHz
12.0	Allow 12.0 Mbps	5-MHz and 10-MHz
13.5	Allow 13.5 Mbps	5-MHz
18.0	Allow 18.0 Mbps	10-MHz
24.0	Allow 24.0 Mbps	10-MHz
27.0	Allow 27.0 Mbps	10-MHz
basic-1.5	Require 1.5 Mbps	5-MHz
basic-2.25	Require 2.25 Mbps	5-MHz
basic-3.0	Require 3 Mbps	5-MHz and 10-MHz
basic-4.5	Require 4.5 Mbps	5-MHz and 10-MHz
basic-6.0	Require 6 Mbps	5-MHz and 10-MHz
basic-9.0	Require 9 Mbps	5-MHz and 10-MHz
basic-12.0	Require 12 Mbps	5-MHz and 10-MHz
basic-13.5	Require 13.5 Mbps	5-MHz
basic-18.0	Require 18 Mbps	10-MHz
basic-24.0	Require 24 Mbps	10-MHz
basic-27.0	Require 27 Mbps	10-MHz
default	Set default rates	Table 9-1 shows the default rates.
range	Set rates for best range	Table 9-1 shows the best range.
throughput	Set rates for best throughput	Table 9-1 shows the best throughput rates.

Table 9-1 Default Rates, Best Range Rates and Best Throughput Rates

5-MHz **Spacing**	**10**-MHz **Spacing**
Default Rates: basic-1.5, 2.25, basic-3.0, 4.5, basic-6.0, 9.0, 12.0, 13.5	Default Rates: basic-3.0, 4.5, basic-6.0, 9.0, basic-12.0, 18.0, 24.0, 27.0

Table 9-1 Default Rates, Best Range Rates and Best Throughput Rates

Rates for Best Range: basic-1.5, 2.25, 3.0, 4.5, 6.0, 9.0, 12.0, 13.5	Rates for Best Range: basic-3.0, 4.5, 6.0 9.0 12.0 18.0 24.0 27.0
Rates for Best Throughput: basic-1.5, basic-2.25, basic-3.0, basic-4.5, basic-6.0, basic-9.0, basic-12.0, basic-13.5	Rates for Best Throughput: basic-3.0, basic-4.5, basic-6.0, basic-9.0, basic-12.0, basic-18.0, basic-24.0, basic-27.0

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 access point 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 access point's MAC address, the WDS access point's IP address, the access point'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** *mac-address*]	On the WDS access point 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'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 access point'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 access point:

Command	Description
debug wlccp ap { **mn** | **mobility** | **rm** | **state** |**wds-discovery** }	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 access point (**state**).
debug wlccp leap-client	Use this command to turn on display of debugging messages related to LEAP-enabled client devices.
debug wlccp packet	Use this command to turn on display of packets to and from the WDS access point.
debug wlccp wds [**state** | **statistics**]	Use this command and the **state** option to turn on display of WDS debug and state messages. Use the **statistics** option to turn on display of failure statistics.

Configuring VLANs

This chapter describes how to configure your WMIC to operate with the VLANs set up on your wired LAN. These sections describe how to configure your WMIC to support VLANs:

- Understanding VLANs, page 10-2
- Configuring VLANs, page 10-4

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 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.

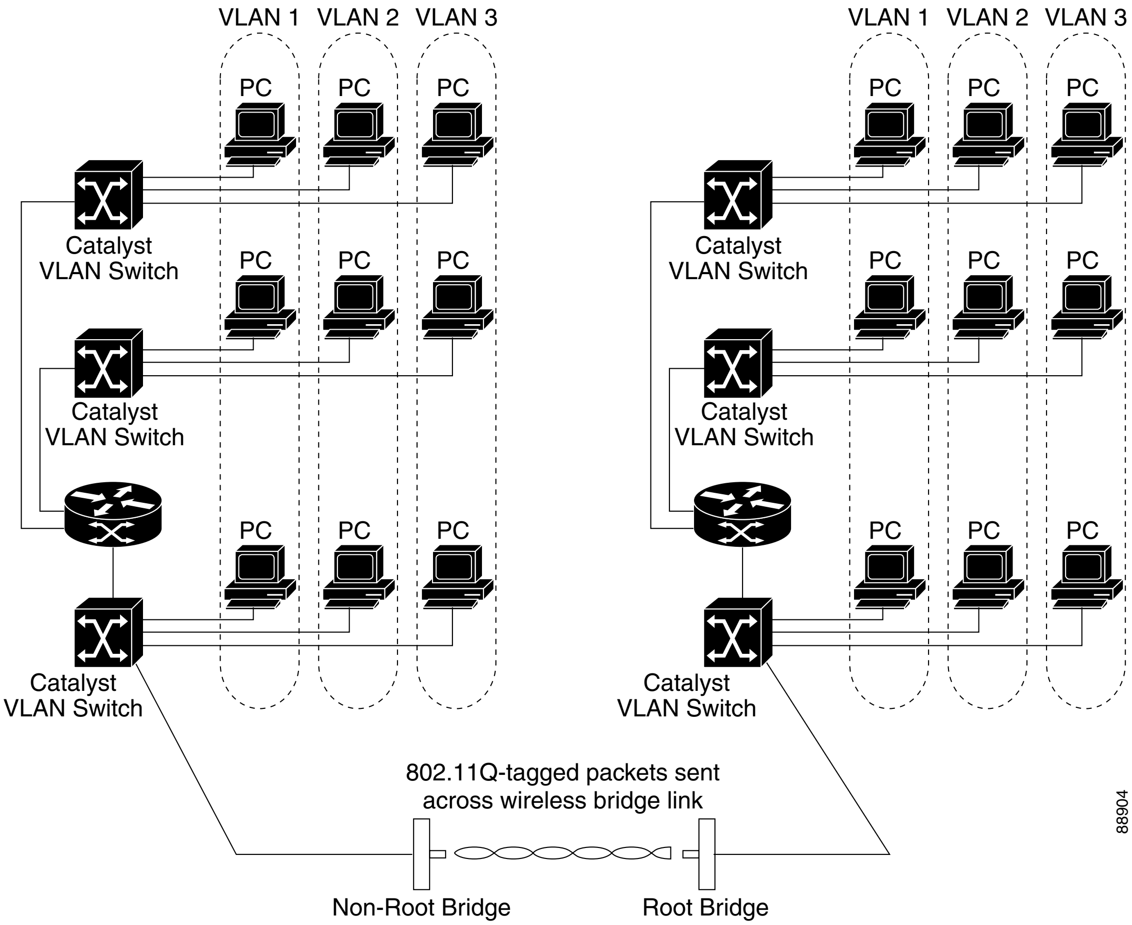
VLANs provide the segmentation services traditionally provided by routers in LAN configurations. VLANs address scalability, security, and network management. You should consider several key issues when designing and building switched LAN networks:

- 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 WMIC. VLAN 802.1Q trunking is supported between root and non-root bridges through the bridges’ primary SSID.

Figure 10-1 shows two bridges sending 802.11Q-tagged packets between two LAN segments that use logical VLAN segmentation.

Figure 10-1 Bridges Connecting LAN Segments Using VLANs



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 Bridges into VLANs

The basic wireless components of a VLAN consist of two or more bridges communicating using wireless technology. The WMIC 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 WMIC's Ethernet port.

In fundamental terms, the key to configuring a WMIC to connect to a specific VLAN is by configuring its SSID to recognize that VLAN. Since VLANs are identified by a VLAN ID, it follows that if the SSID on a WMIC is configured to recognize a specific VLAN ID, a connection to the VLAN is established.

The WMIC supports 16 SSIDs. You can assign only one SSID to the native VLAN.

Configuring VLANs

These sections describe how to configure VLANs on your WMIC:

- Configuring a VLAN, page 10-4
- Viewing VLANs Configured on the WMIC, page 10-7

Configuring a VLAN

Configuring your WMIC 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 a bridge group to each VLAN.
4. (Optional) Enable WEP on the native VLAN.
5. Assign the WMIC'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 WMIC radio and Ethernet ports. For detailed instructions on assigning authentication types to SSIDs, see Chapter 8, "Configuring Authentication Types."

Beginning in privileged EXEC mode, follow these steps to assign an SSID to a VLAN and enable the VLAN on the WMIC 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** *vlan-id* [**native**]	Enable a VLAN on the subinterface. (Optional) Designate the VLAN as the native VLAN. On many networks, the native VLAN is VLAN 1.

	Command	Purpose
Step 4	**bridge-group** *number*	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 WMIC enables the subinterface to be ready to participate in STP when you enter the **bridge** *n* **protocol ieee** command. See Chapter 6, "Configuring Spanning Tree Protocol," for complete instructions on enabling STP on the WMIC.
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** *vlan-id* [**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** *number*	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** *ssid-string*	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 up to 16 SSIDs on the bridge; however, only one SSID can be assigned to the native VLAN. **Note** You use the **ssid** command's authentication options to configure an authentication type for each SSID. See Chapter 8, "Configuring Authentication Types," for instructions on configuring authentication types.
Step 12	**vlan** *vlan-id*	Assign the SSID to the native VLAN.
Step 13	**infrastructure-ssid**	Designate the SSID as the infrastructure SSID. It is used to instruct a non-root bridge or workgroup bridge radio to associate with this SSID.

	Command	Purpose
Step 14	**encryption** [**vlan** *vlan-id*] **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 bridge can associate to the WMIC with or without WEP enabled. You can enable TKIP with WEP set to optional but you cannot enable MIC. If you enter **mandatory**, other bridges must have WEP enabled to associate to the WMIC. You can enable both TKIP and MIC with WEP set to mandatory. **Note** You can enable encryption for each VLAN, but the WMIC 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 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

```
bridge# configure terminal
bridge(config)# interface dot11radio0.1
bridge(config-subif)# encapsulation dot1q 1 native
bridge(config-subif)# bridge group 1
bridge(config-subif)# exit
bridge(config)# interface fastEthernet0.1
bridge(config-subif)# encapsulation dot1q 1 native
bridge(config-subif)# bridge group 1
bridge(config-subif)# exit
bridge(config)# interface dot11radio0
bridge(config-if)# ssid batman
bridge(config-ssid)# vlan 1
bridge(config-ssid)# infrastructure-ssid
bridge(config-ssid)# end
```

Viewing VLANs Configured on the WMIC

In privileged EXEC mode, use the **show vlan** command to view the VLANs that the WMIC 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:
```

CHAPTER 11

Configuring QoS in a Wireless Environment

This chapter describes how to configure quality of service (QoS) on your WMIC. With this feature, you can provide preferential treatment to certain traffic at the expense of others. Without QoS, the WMIC 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.

This chapter consists of these sections:

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 WMIC, 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 WMIC. If you do not use VLANs on your network, you can apply your QoS policies to the WMIC's Ethernet and radio ports.

Note Configuring the limited WMIC QoS features typically are not enough to manage the traffic when traffic can congest the limited 20 Mbps bandwidth of the WMIC. We highly recommended that you apply traffic shaping and other MQC based QoS features.

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, bridges 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 match packets using ACL; they use only MQC class-map for matching clauses.
- 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. Bridges do not support ISL.
- They support only MQC policy-map **set cos** action.

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 WMIC 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 WMIC. These are the effects of QoS on network traffic:

- The radio downstream flow is traffic transmitted out the WMIC radio to another bridge. This traffic is the main focus for QoS on a wireless LAN.
- The radio upstream flow is traffic received on the WMIC radio from another bridge. QoS for wireless LAN does not affect this traffic.
- The Ethernet downstream flow is traffic sent from a switch or a router to the Ethernet port on the WMIC. If QoS is enabled on the switch or router, the switch or router might prioritize and rate-limit traffic to the WMIC.
- The Ethernet upstream flow is traffic sent from the WMIC Ethernet port to a switch or router on the wired LAN. The WMIC does not prioritize traffic that it sends to the wired LAN based on traffic classification.

Precedence of QoS Settings

When you enable QoS, the WMIC queues packets based on the Layer 2 class of service value for each packet. The WMIC applies QoS policies in this order:

1. Packets already classified—When the WMIC 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 WMIC 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 WMIC.

Note The WMIC always acts on tagged 802.1P packets that it receives over the radio interface, even if a QoS policy has not been configured.

2. Policies you create on the WMIC—QoS Policies that you create and apply to VLANs or to the WMIC interfaces are second in precedence after previously classified packets.
3. 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.

Configuring QoS

QoS is disabled by default. This section describes how to configure QoS on your WMIC. It contains this configuration information:

- Configuration Guidelines, page 11-4
- Configuring QoS Using the Web-Browser Interface, page 11-4
- Adjusting Radio Access Category Definitions, page 11-7

Configuration Guidelines

Before configuring QoS on your WMIC, 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

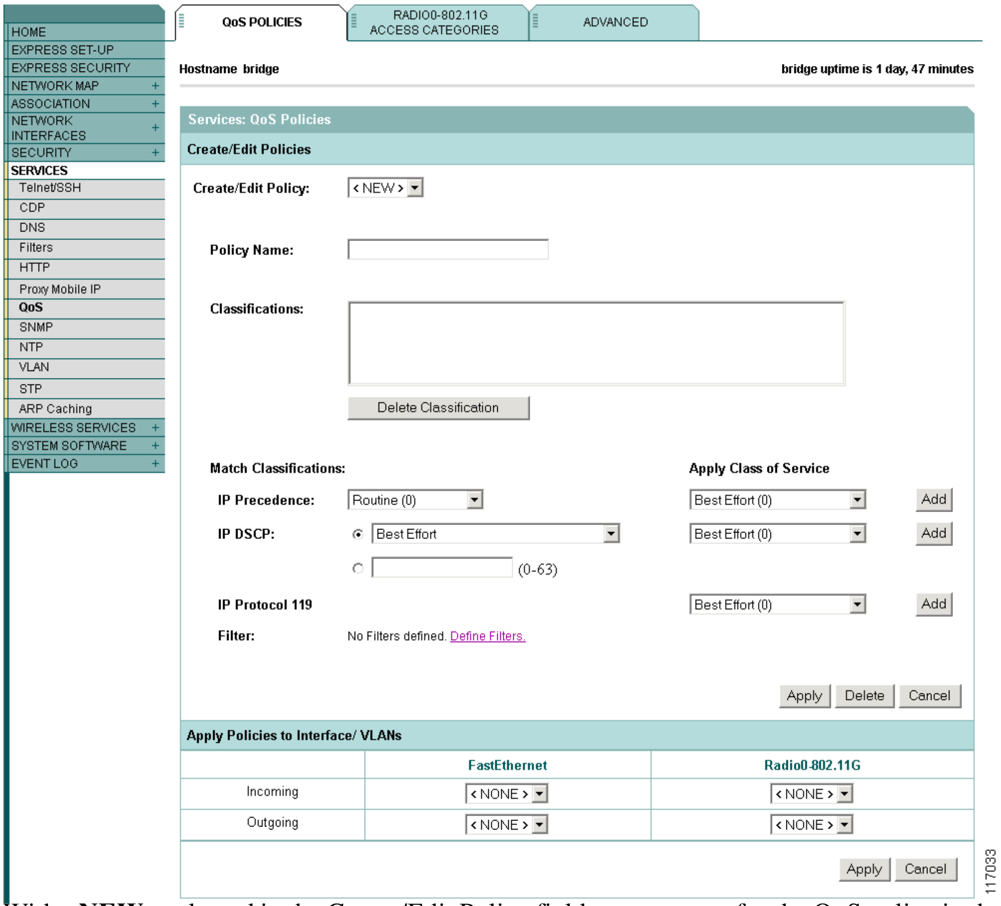
This section describes configuring QoS using the web-browser interface.

Follow these steps to configure QoS:

Step 1 If you use VLANs on your wireless LAN, make sure the necessary VLAN is configured on your WMIC before configuring QoS.

Step 2 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 11-1 shows the QoS Policies page.

Figure 11-1 QoS Policies Page



Hostname bridge

bridge uptime is 1 day, 47 minutes

Create/Edit Policy: < NEW >

Policy Name:

Classifications:

IP Precedence: Routine (0) Best Effort (0)

IP DSCP: ● Best Effort Best Effort (0)

○ (0-63)

IP Protocol 119 Best Effort (0)

Filter: No Filters defined. Define Filters.

	FastEthernet	Radio0-802.11G
Incoming	< NONE >	< NONE >
Outgoing	< NONE >	< NONE >

Step 3 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 4 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 5 Use the Apply Class of Service drop-down menu to select the class of service that the WMIC will apply to packets of the type that you selected from the IP Precedence menu. The WMIC 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 <10ms Latency (6)
- Network Control (7)

Step 6 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 7 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 8 Use the Apply Class of Service drop-down menu to select the class of service that the WMIC will apply to packets of the type that you selected from the IP DSCP menu. The WMIC matches your IP DSCP selection with your class of service selection.

Step 9 Click the **Add** button beside the Class of Service menu for IP DSCP. The classification appears in the Classifications field.

Step 10 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 WMIC, 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 WMIC's packet forwarding decisions.

Step 11 Use the Apply Class of Service drop-down menu to select the class of service that the WMIC will apply to packets that match the filter that you selected from the Filter menu. The WMIC matches your filter selection with your class of service selection.

Step 12 Click the **Add** button beside the Class of Service menu for Filter. The classification appears in the Classifications field.

Step 13 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 WMIC will apply to all packets on a VLAN. The WMIC matches all packets with your class of service selection.

Step 14 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 15 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 16 Use the Apply Policies to Interface/VLANs drop-down menus to apply policies to the Ethernet and radio ports. If VLANs are configured on the WMIC, drop-down menus for each VLAN's virtual ports appear in this section. If VLANs are not configured on the WMIC, drop-down menus for each interface appear.

Step 17 Click the **Apply** button at the bottom of the page to apply the policies to the ports.

Adjusting Radio Access Category Definitions

The WMIC uses the radio access category definitions 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.

We strongly recommend that you use the default settings on the Radio Traffic Access Categories page, or that you use the settings described in section x. 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 11-1.

The values listed in Table 11-1 are to the power of 2. The WMIC computes Contention Window values with this equation:

CW = 2 ** X minus 1

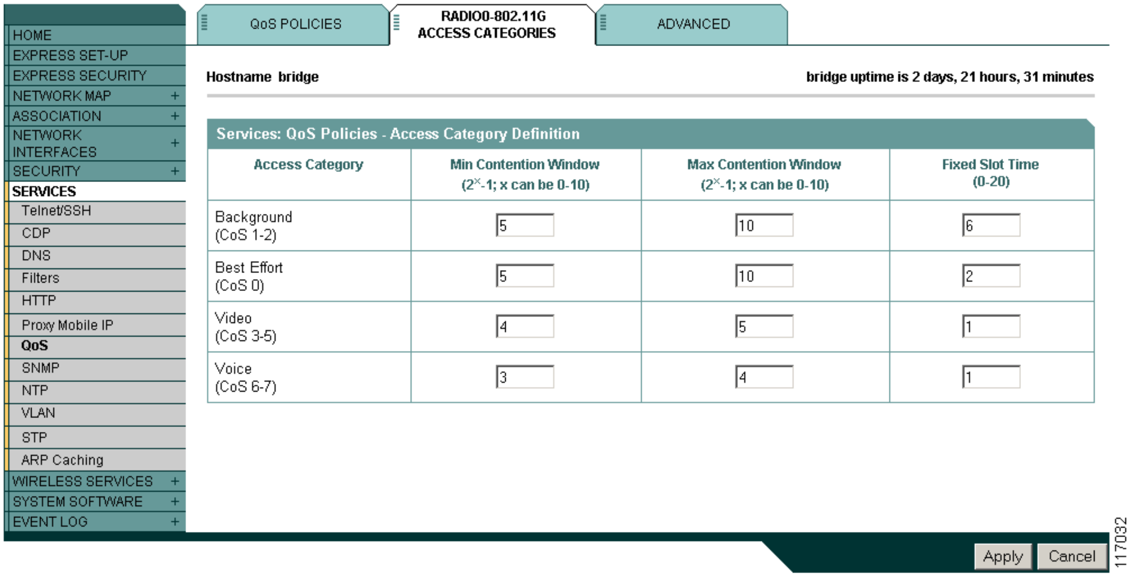
where X is the value from Table 11-1.

Table 11-1 Default QoS Radio Traffic Class Definitions

Class of Service	Min Contention Window	Max Contention Window	Fixed Slot Time
Background (CoS 1-2)	5	10	6
Best Effort (CoS 0)	5	10	2
Video (CoS 3-5)	5	10	2
Voice (CoS 6-7)	3	4	1

Figure 11-2 shows the Radio 802.11G Access Categories page.

Figure 11-2 Radio 802.11G Access Categories Page



Hostname bridge

bridge uptime is 2 days, 21 hours, 31 minutes

Services: QoS Policies - Access Category Definition

Access Category	Min Contention Window (2^x-1; x can be 0-10)	Max Contention Window (2^x-1; x can be 0-10)	Fixed Slot Time (0-20)
Background (CoS 1-2)	5	10	6
Best Effort (CoS 0)	5	10	2
Video (CoS 3-5)	4	5	1
Voice (CoS 6-7)	3	4	1

CW-min and CW-max Settings for Point-to-Point and Point-to-Multipoint Bridge Links

For best performance on your WMIC links, adjust the CW-min and CW-max contention window settings according to the values listed in Table 11-2. 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 disabled by default.

Table 11-2 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** *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 11-2 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:

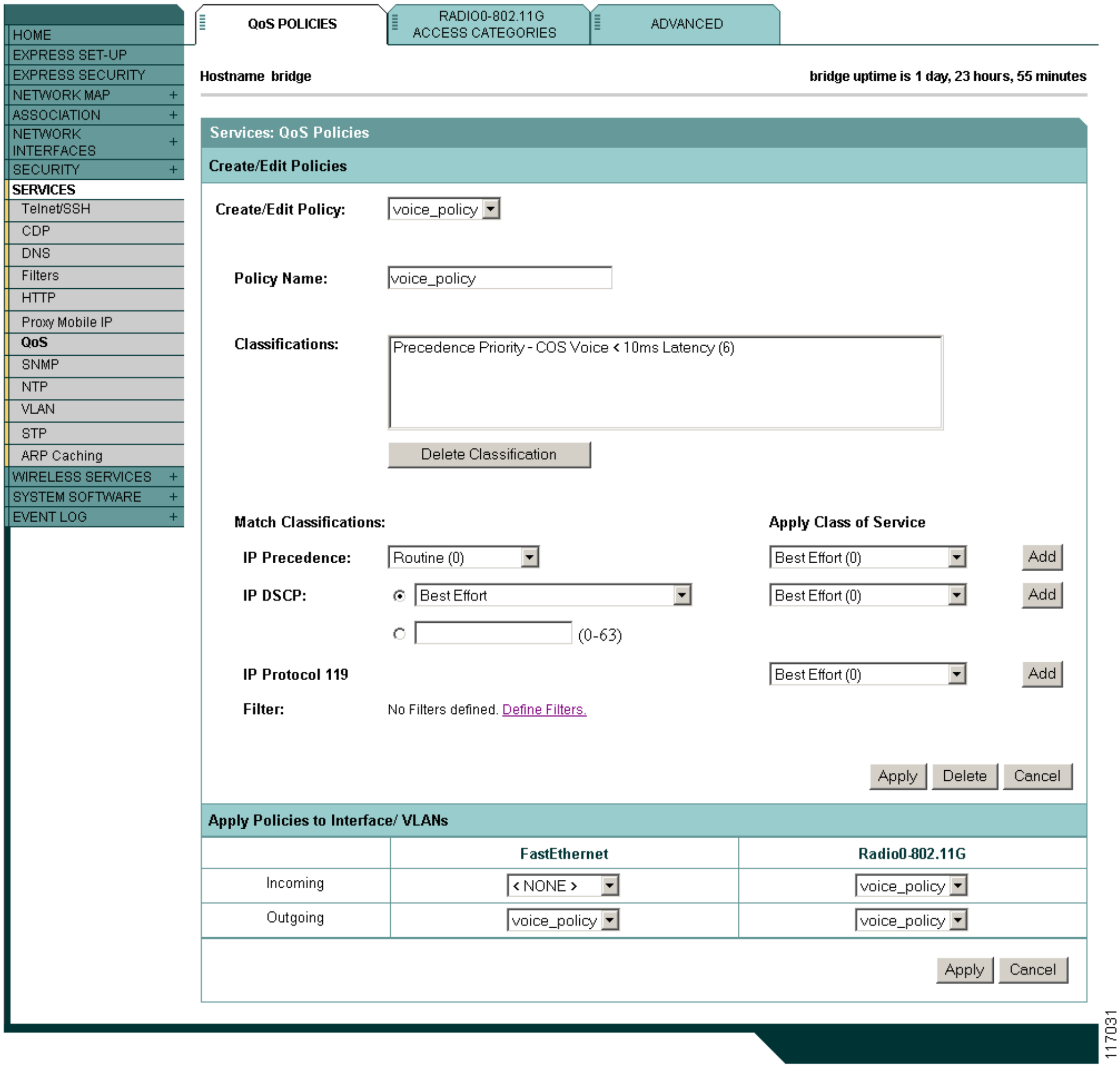
- Giving Priority to Voice Traffic, page 11-9
- Giving Priority to Video Traffic, page 11-10

Giving Priority to Voice Traffic

This section demonstrates how you can apply a QoS policy to your wireless network.

In this example, the network administrator creates a policy named *voice_policy* that applies voice class of service to traffic from packets having Priority precedence in IP Precedence field. The user applies the voice_policy to the incoming and outgoing radio ports and to the outgoing Ethernet port. Figure 11-3 shows the administrator’s QoS Policies page.

Figure 11-3 QoS Policies Page for Voice Example



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)

Match Classifications:		Apply Class of Service
IP Precedence:	Routine (0)	Best Effort (0)
IP DSCP:	● Best Effort	Best Effort (0)
	○ (0-63)	
IP Protocol 119		Best Effort (0)
Filter:	No Filters defined. Define Filters.	

Apply Policies to Interface/ VLANs

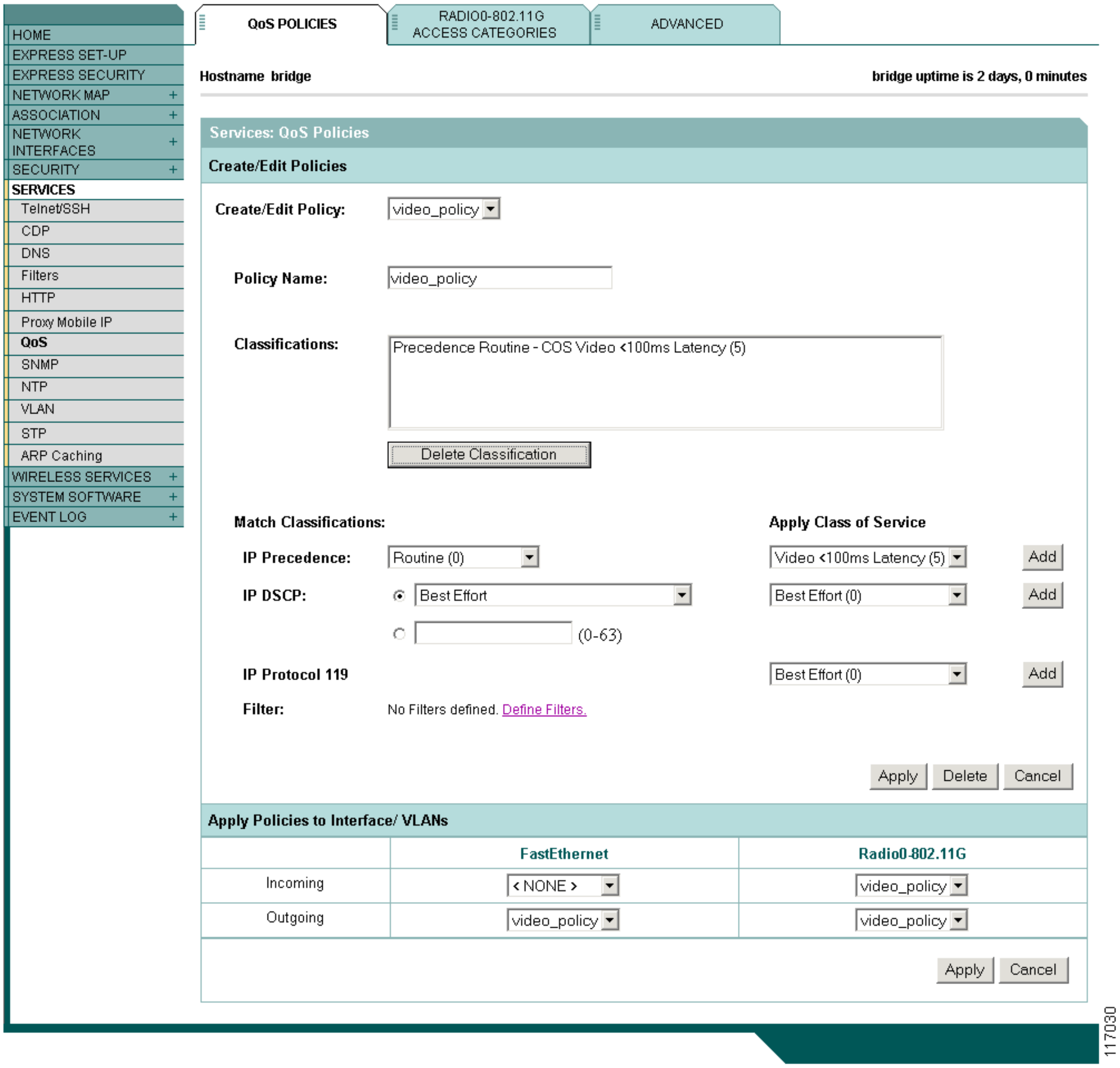
	FastEthernet	Radio0-802.11G
Incoming	< NONE >	voice_policy
Outgoing	voice_policy	voice_policy

Giving Priority to Video Traffic

This section demonstrates how you could apply a QoS policy to a 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. Figure 11-4 shows the administrator’s QoS Policies page.

Figure 11-4 QoS Policies Page for Video Example



Hostname bridge

bridge uptime is 2 days, 0 minutes

Create/Edit Policy: video_policy

Policy Name: video_policy

Classifications: Precedence Routine - COS Video <100ms Latency (5)

	Match Classifications	Apply Class of Service
IP Precedence:	Routine (0)	Video <100ms Latency (5)
IP DSCP:	● Best Effort ○ (0-63)	Best Effort (0)
IP Protocol 119		Best Effort (0)
Filter:	No Filters defined. Define Filters.	

	FastEthernet	Radio0-802.11G
Incoming	< NONE >	video_policy
Outgoing	video_policy	video_policy

QoS Example Configuration for VLAN

The example in this section queues all traffic from VLAN100 to the voice queue.

```
interface fastEthernet 0.1
 encapsulation dot1Q 1 native
 bridge-group 1

interface fastEthernet 0.100
 encapsulation dot1Q 100
 bridge-group 100

interface fastEthernet 0.101
 encapsulation dot1Q 101
 bridge-group 101
```

```
interface dot11Radio 0.1
 encapsulation dot1Q 1 native
 bridge-group 1

interface dot11Radio 0.100
 encapsulation dot1Q 100
 bridge-group 100

interface dot11Radio 0.101
 encapsulation dot1Q 101
 bridge-group 101

interface dot11Radio 0
 ssid qosWMIC-1
  vlan 1
  authentication open
 ssid qosWMIC-100
  vlan 100
  authentication open
 ssid qosWMIC-101
  vlan 101
  authentication open

class-map match-all alldata
 match any

policy-map v100traffic
 class alldata
  set cos 6

interface dot11Radio 0.100
 service-policy output v100traffic
```

QoS Example of IP DSCP and IP Precedence

The example in this section queues traffic data with the IP Precedence value 2 to Queue 0, IP DSCP value 12 to Queue 1, IP Precedence value 5 to Queue 2, and IP DSCP value 46 to queue 3.

```
class-map match-all dscp12
 match ip dscp af12

class-map match-all dscp46
 match ip dscp ef

class-map match-all prec2
 match ip precedence immediate

class-map match-all prec5
 match ip precedence critical

policy-map L3Map
class prec2
  set cos 2
 class dscp12
  set cos 0
class prec5
  set cos 5
class dscp46
  set cos 6

interface dot11Radio 0
 service-policy output L3Map
```

CHAPTER 12

Configuring Filters

This chapter describes how to configure and manage MAC address, IP, and Ethertype filters on the WMIC using the web-browser interface. This chapter contains these sections:

Understanding Filters

Protocol filters (IP protocol, IP port, and Ethertype) prevent or allow the use of specific protocols through the WMIC'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 WMIC's radio port prevents SNMP access through the radio 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 WMIC's QoS policies. Refer to Chapter 11, "Configuring QoS in a Wireless Environment," 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 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/bcfpart1/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/l3sw/4908g_l3/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 12-3
- Configuring and Enabling IP Filters, page 12-5
- Configuring and Enabling Ethertype Filters, page 12-7

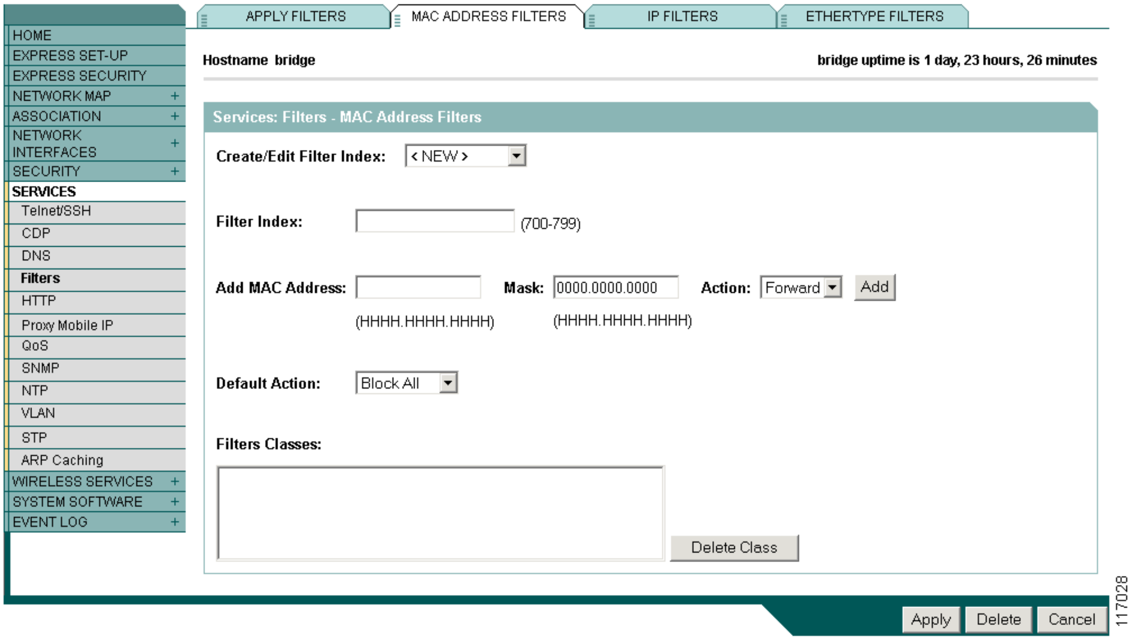
Configuring and Enabling MAC Address Filters

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 MAC address filters are powerful, and you can lock yourself out of the WMIC if you make a mistake setting up the filters. If you accidentally lock yourself out of your WMIC, use the CLI to disable the filters, or reset the WMIC to factory defaults.

Use the MAC Address Filters page to create MAC address filters for the WMIC. Figure 12-1 shows the MAC Address Filters page.

Figure 12-1 MAC Address Filters Page



Hostname bridge

bridge uptime is 1 day, 23 hours, 26 minutes

Services: Filters - MAC Address Filters

Create/Edit Filter Index: < NEW >

Filter Index: (700-799)

Add MAC Address: (HHHH.HHHH.HHHH) Mask: 0000.0000.0000 (HHHH.HHHH.HHHH) Action: Forward

Default Action: Block All

Filters Classes:

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 (0040.9612.3456, for example).

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 **FFFF.FFFF.FFFF**. To check only the first 4 bytes, enter **FFFF.FFFF.0000**.

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**.

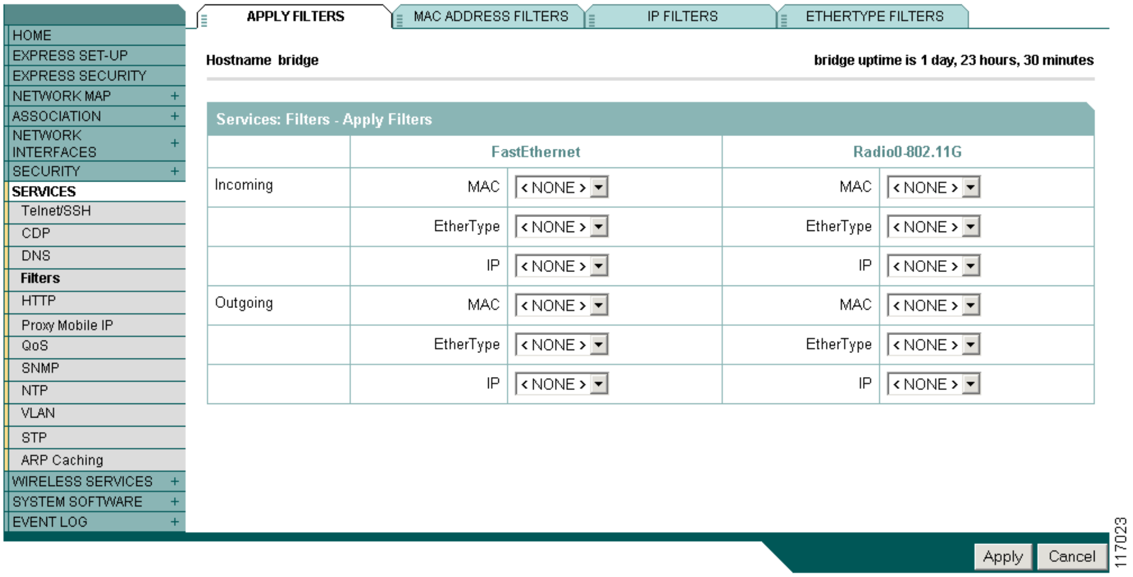
Step 8 Repeat Step 4 through Step 7 to add addresses to the filter.

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.

Step 10 Click **Apply**. The filter is saved on the WMIC, 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 12-2 shows the Apply Filters page.

Figure 12-2 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 >

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.

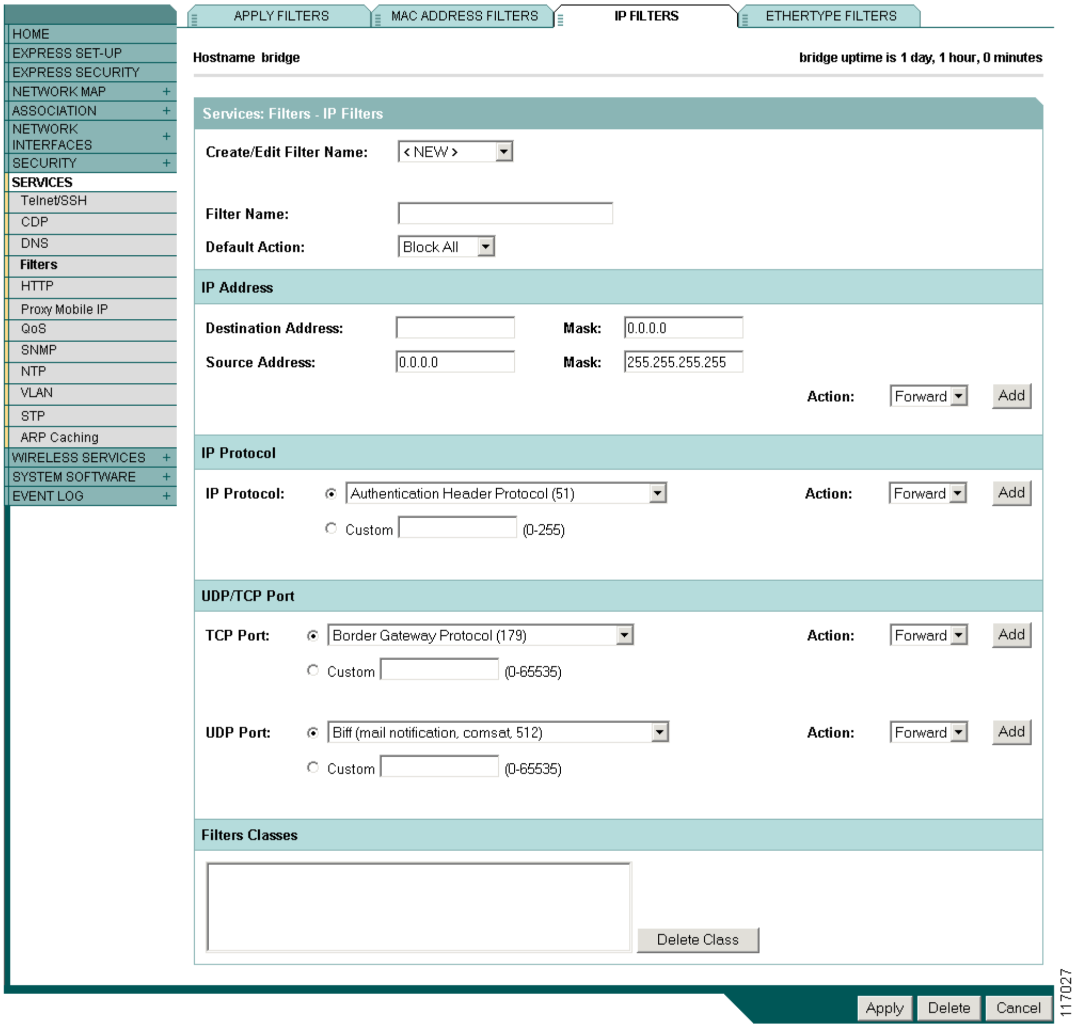
Step 13 Click **Apply**. The filter is enabled on the selected ports.

Configuring and Enabling IP Filters

IP filters (IP address, IP protocol, and IP port) prevent or allow the use of specific protocols through the WMIC'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 WMIC. Figure 12-3 shows the IP Filters page.

Figure 12-3 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

IP Protocol

IP Protocol: ● Authentication Header Protocol (51) Action: Forward

○ Custom (0-255)

UDP/TCP Port

TCP Port: ● Border Gateway Protocol (179) Action: Forward

○ Custom (0-65535)

UDP Port: ● Biff (mail notification, comsat, 512) Action: Forward

○ Custom (0-65535)

Filters Classes

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 WMIC.

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 WMIC accepts any IP address. If you enter 0.0.0.0, the WMIC 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 WMIC.

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 C, "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 WMIC.

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 C, "Protocol Filters," for a list of IP port protocols and their numeric designators.

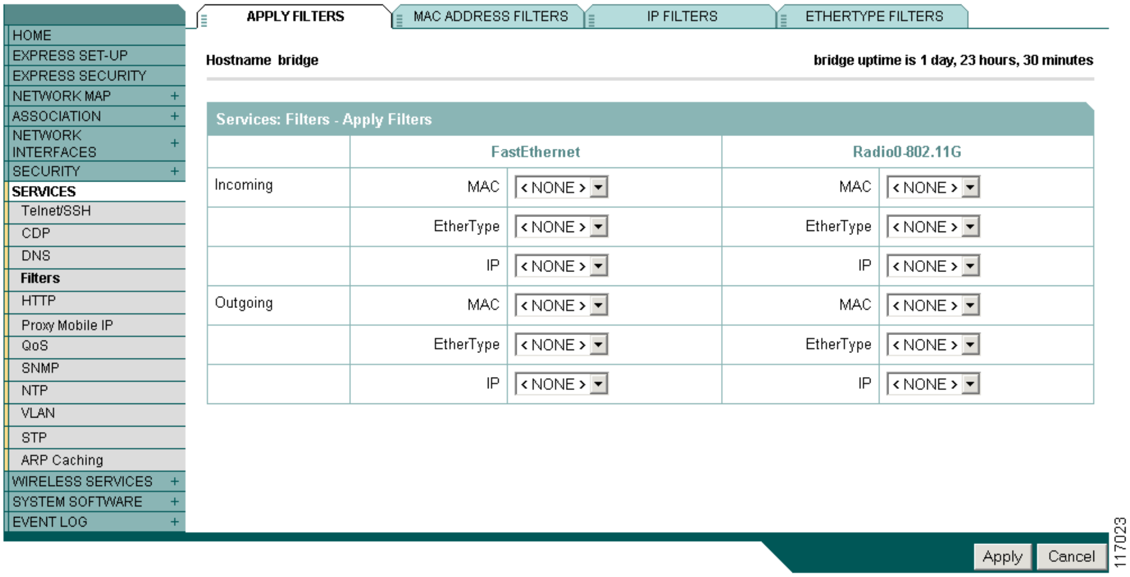
Step 13 Select **Forward** or **Block** from the Action menu.

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 WMIC, 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 12-4 shows the Apply Filters page.

Figure 12-4 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 >

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.

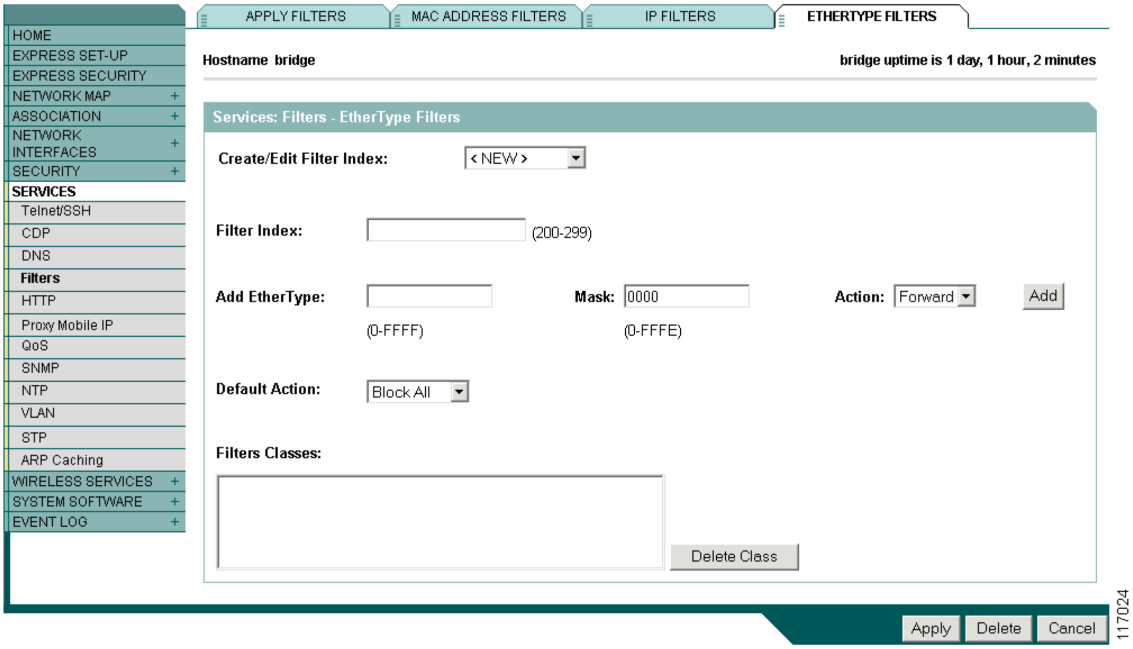
Step 18 Click **Apply**. The filter is enabled on the selected ports.

Configuring and Enabling Ethertype Filters

Ethertype filters prevent or allow the use of specific protocols through the WMIC'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. Figure 12-5 shows the Ethertype Filters page.

Figure 12-5 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: 0000 (0-FFFE)

Action: Forward

Default Action: Block All

Filters Classes:

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 C, "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.

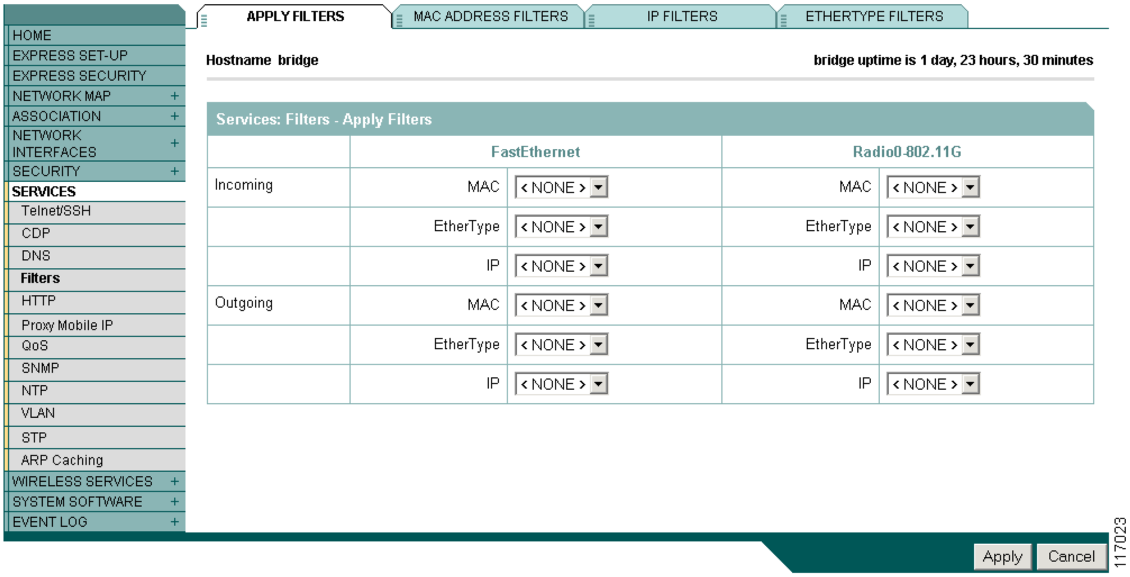
Step 7 Click **Add**. The Ethertype appears in the Filters Classes field. To remove the Ethertype from the Filters Classes list, select it and click **Delete Class**. Repeat Step 4 through Step 7 to add Ethertypes to the filter.

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 WMIC, 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 12-6 shows the Apply Filters page.

Figure 12-6 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 >

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 WMIC.

This chapter contains these sections:

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 WMIC's Ethernet and radio ports by default.

Note For best performance on your wireless LAN, disable CDP on all radio interfaces and on sub-interfaces if VLANs are enabled on the WMIC.

Configuring CDP

This section contains CDP configuration information and procedures:

- Default CDP Configuration, page 13-2
- Configuring the CDP Characteristics, page 13-3
- Disabling and Enabling CDP, page 13-3
- Disabling and Enabling CDP on an Interface, page 13-4

Default CDP Configuration

Table 13-1 lists the default CDP settings.

Table 13-1 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 WMIC discards CDP packets) and the CDP timer (the number of seconds between each CDP packets the WMIC 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** *seconds*	(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** *seconds*	(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:

```
bridge# configure terminal
bridge(config)# cdp holdtime 120
bridge(config)# cdp timer 50
bridge(config)# end

bridge# 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 13-5.

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.

```
bridge# configure terminal
bridge(config)# cdp run
bridge(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** *interface-id*	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** *interface-id*	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:

```
bridge# configure terminal
bridge(config)# interface x
bridge(config-if)# cdp enable
bridge(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 *entry-name* [**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 [*type number*]	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 [*type number*] [**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:

```
bridge# show cdp
Global CDP information:
        Sending CDP packets every 50 seconds
        Sending a holdtime value of 120 seconds

bridge# show cdp entry *
-------------------------
Device ID: bridge
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
0FFFFFFFF010221FF000000000000000024B293A00FF0000
VTP Management Domain: ''
Duplex: full

-------------------------
Device ID: idf2-1-lab-l3.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
0FFFFFFFF010101FF000000000000000142EFA400FF
VTP Management Domain: ''

bridge# 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

bridge# 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

bridge# 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

bridge# 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 WMIC.

This chapter consists of these sections:

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 WMIC. To configure SNMP on the WMIC, 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 14-2
- SNMP Manager Functions, page 14-3
- SNMP Agent Functions, page 14-3
- SNMP Community Strings, page 14-4
- Using SNMP to Access MIB Variables, page 14-4

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.

SNMPv2C replaces the Party-based Administrative and Security Framework of SNMPv2Classic with the Community-based Administrative Framework of SNMPv2C while retaining the bulk retrieval and improved error handling of SNMPv2Classic.

Both SNMPv1 and SNMPv2C use a community-based form of security. The community of managers able to access the agent's MIB is defined by an IP address access control list and password.

SNMPv2C includes a bulk retrieval mechanism and more detailed error message reporting to management stations. The bulk retrieval mechanism retrieves tables and large quantities of information, minimizing the number of round-trips required. The SNMPv2C improved error-handling includes expanded error codes that distinguish different kinds of error conditions; these conditions are reported through a single error code in SNMPv1. Error return codes now report the error type.

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 SNMPv1 protocol and another using the SNMPv2 protocol.

SNMP Manager Functions

The SNMP manager uses information in the MIB to perform the operations described in Table 14-1.

Table 14-1 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 WMIC, the community string definitions on the NMS must match at least one of the three community string definitions on the WMIC.

A community string can have one of these attributes:

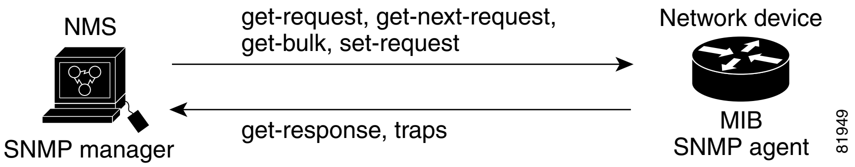
- Read-only—Gives read access to authorized management stations to all objects in the MIB except the community strings, but does not allow write access
- Read-write—Gives read and write access to authorized management stations to all objects in the MIB, but does not allow access to the community strings

Using SNMP to Access MIB Variables

An example of an NMS is the CiscoWorks network management software. CiscoWorks 2000 software uses the 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 14-1, 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 14-1 SNMP Network



For information on supported MIBs and how to access them, see Appendix D, “Supported MIBs.”

Configuring SNMP

This section describes how to configure SNMP on your WMIC. It contains this configuration information:

- Default SNMP Configuration, page 14-5
- Enabling the SNMP Agent, page 14-5
- Configuring Community Strings, page 14-5
- Configuring Trap Managers and Enabling Traps, page 14-7
- Setting the Agent Contact and Location Information, page 14-10
- Using the snmp-server view Command, page 14-10
- SNMP Examples, page 14-10

Default SNMP Configuration

Table 14-2 shows the default SNMP configuration.

Table 14-2 Default SNMP Configuration

Feature	Default Setting
SNMP agent	Disabled
SNMP community strings	None configured
SNMP trap receiver	None configured
SNMP traps	None enabled

Enabling the SNMP Agent

No specific IOS 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 WMIC.

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 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 IOS software.

Beginning in privileged EXEC mode, follow these steps to configure a community string on the WMIC:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**snmp-server community** *string* [*access-list-number*] [**view** *mib-view*] [**ro** | **rw**]	Configure the community string. • For *string*, 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 *access-list-number*, enter an IP standard access list numbered from 1 to 99 and 1300 to 1999. • (Optional) For **view** *mib-view*, specify a MIB view to which this community has access, such as **ieee802dot11**. See the "Using the snmp-server view Command" section on page 14-10 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** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	(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 *access-list-number*, 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 *source*, enter the IP address of the SNMP managers that are permitted to use the community string to gain access to the agent. • (Optional) For *source-wildcard*, 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:

```
bridge(config)# snmp-server view dot11view ieee802dot11 included
bridge(config)# snmp-server community open rw
bridge(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 device generates when certain events occur. By default, no trap manager is defined, and no traps are issued.

Bridges running this IOS release can have an unlimited number of trap managers. Community strings can be any length.

Table 14-3 describes the supported traps (notification types). You can enable any or all of these traps and configure a trap manager to receive them.

Table 14-3 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.
envmon temperature	Enable traps for monitoring radio temperature. This trap is sent out when the WMIC radio temperature approaches the limits of its operating range.
snmp	Enable traps for SNMP events.
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 14-3.

Beginning in privileged EXEC mode, follow these steps to configure the WMIC to send traps to a host:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**snmp-server host** *host-addr* {**traps** | **informs**} {**version** {**1** | **2c**}} *community-string notification-type*	Specify the recipient of the trap message. • For *host-addr,* 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. **Note** Though visible in the command-line help string, the **version 3** keyword (SNMPv3) is not supported. • For *community-string,* specify the string to send with the notification operation. Though you can set this string using the **snmp-server host** command, we recommend that you define this string by using the **snmp-server community** command before using the **snmp-server host** command. • For *notification-type*, use the keywords listed in Table 14-3 on page 14-8.
Step 3	**snmp-server enable traps** *notification-types*	Enable the WMIC to send specific traps. For a list of traps, see Table 14-3 on page 14-8. 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** *text*	Set the system contact string. For example: `snmp-server contact Dial System Operator at beeper 21555.`
Step 3	**snmp-server location** *text*	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:

```
bridge(config)# snmp-server view ieee ieee802dot11 included
bridge(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 WMIC to send any traps.

```
bridge(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:

```
bridge(config)# snmp-server view dot11view ieee802dot11 included
bridge(config)# snmp-server community open rw
bridge(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 WMIC 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.

```
bridge(config)# snmp-server community public
bridge(config)# snmp-server enable traps config
bridge(config)# snmp-server host 192.180.1.27 version 2c public
bridge(config)# snmp-server host 192.180.1.111 version 1 public
bridge(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*.

```
bridge(config)# snmp-server community comaccess ro 4
bridge(config)# snmp-server enable traps snmp authentication
bridge(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 WMIC 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*.

```
bridge(config)# snmp-server enable traps entity
bridge(config)# snmp-server host cisco.com restricted entity
```

This example shows how to enable the WMIC to send all traps to the host *myhost.cisco.com* using the community string *public*:

```
bridge(config)# snmp-server enable traps
bridge(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 12.2*.

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.

This chapter consists of these sections:

Working with the Flash File System

The Flash file system on your WMIC 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 15-2
- Setting the Default File System, page 15-3
- Displaying Information About Files on a File System, page 15-3
- Changing Directories and Displaying the Working Directory, page 15-4
- Creating and Removing Directories, page 15-4
- Copying Files, page 15-5
- Deleting Files, page 15-5
- Creating, Displaying, and Extracting tar Files, page 15-6
- Displaying the Contents of a File, page 15-8

Displaying Available File Systems

To display the available file systems on your WMIC, use the **show file systems** privileged EXEC command as shown in this example:

```
bridge# 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   rcp:
           -           -   network     rw   ftp:
```

Table 15-1 lists field descriptions for the **show file systems** command.

Table 15-1 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 15-1 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. **nvram**—The file system is for a nonvolatile RAM (NVRAM) device. **opaque**—The file system is a locally generated *pseudo* file system (for example, the *system*) 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. **nvram:**—Non-volatile RAM memory (NVRAM). **null:**—Null destination for copies. You can copy a remote file to null to determine its size. **rcp:**—Remote Copy Protocol (RCP) network server. **system:**—Contains the system memory, including the running configuration. **tftp:**—Trivial File Transfer Protocol (TFTP) network server. **zflash:**—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 15-2:

Table 15-2 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 *filesystem***:**, 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 *new_configs*.
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 *filesystem***:**, 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 *old_configs*. 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 15-8.

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 15-19.

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 WMIC 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:

```
bridge# 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:

```
bridge# 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
  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 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:

```
bridge# archive tar /table flash:c1200-k9w7-mx.122-8.JA.tar
info (219 bytes)
c1400-k9w7-mx.122-11.JA/ (directory)
c1400-k9w7-mx.122-11.JA/html/ (directory)
c1400-k9w7-mx.122-11.JA/html/foo.html (0 bytes)
c1400-k9w7-mx.122-11.JA/c1200-k9w7-mx.122-8.JA.bin (610856 bytes)
c1400-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:

```
bridge# archive tar /table flash:c1200-k9w7-mx.122-8.JA/html
c1400-k9w7-mx.122-11.JA/html/ (directory)
c1400-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
  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 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.

```
bridge# 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:

```
bridge# more tftp://serverA/hampton/savedconfig
!
! Saved configuration on server
!
version 11.3
service timestamps log datetime localtime
service linenumber
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 WMIC 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 WMIC for various reasons:

- To restore a backed-up configuration file.
- To use the configuration file for another bridge. For example, you might add another bridge to your network and want it to have a configuration similar to the original bridge. By copying the file to the new 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 WMIC 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

Creating configuration files can aid in your WMIC 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 WMIC, you must set them on each 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 WMIC 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 WMIC as if you were entering the commands at the command line. The WMIC 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 WMIC.

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 a WMIC to a server.

For more information, see the "Downloading the Configuration File by Using TFTP" section on page 15-11, the "Downloading a Configuration File by Using FTP" section on page 15-13, or the "Downloading a Configuration File by Using RCP" section on page 15-16.

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 WMIC by using configuration files you create, download from another device, 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 15-10
- Downloading the Configuration File by Using TFTP, page 15-11
- Uploading the Configuration File by Using TFTP, page 15-11

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 WMIC has a route to the TFTP server. The WMIC 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 WMIC 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 15-10.

Step 3 Log into the WMIC through a Telnet session.

Step 4 Download the configuration file from the TFTP server to configure the WMIC.

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-confg* at IP address 172.16.2.155:

```
bridge# copy tftp://172.16.2.155/tokyo-confg system:running-config
Configure using tokyo-confg from 172.16.2.155? [confirm] y
Booting tokyo-confg from 172.16.2.155:!!! [OK - 874/16000 bytes]
```

Uploading the Configuration File by Using TFTP

To upload a configuration file from a WMIC 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 15-10.

Step 2 Log into the WMIC through a Telnet session.

Step 3 Upload the WMIC 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 WMIC to a TFTP server:

```
bridge# copy system:running-config tftp://172.16.2.155/tokyo-config
Write file tokyo-confg on host 172.16.2.155? [confirm] y
#
Writing tokyo-confg!!! [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 WMIC 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 WMIC 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 WMIC 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 WMIC.

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

Before you begin downloading or uploading a configuration file by using FTP, perform these tasks:

- Ensure that the WMIC has a route to the FTP server. The WMIC 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 WMIC 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 WMIC 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 WMIC.

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 15-13.
Step 2		Log into the WMIC through a Telnet session.
Step 3	**configure terminal**	Enter global configuration mode on the WMIC. 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** *username*	(Optional) Change the default remote username.
Step 5	**ip ftp password** *password*	(Optional) Change the default password.
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-confg* 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 WMIC:

```
bridge# copy ftp://netadmin1:mypass@172.16.101.101/host1-confg system:running-config
Configure using host1-confg from 172.16.101.101? [confirm]
```

```
Connected to 172.16.101.101
Loading 1112 byte file host1-confg:![OK]
bridge#
%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-confg* from the *netadmin1* directory on the remote server with an IP address of 172.16.101.101 to the WMIC startup configuration.

```
bridge# configure terminal
bridge(config)# ip ftp username netadmin1
bridge(config)# ip ftp password mypass
bridge(config)# end
bridge# copy ftp: nvram:startup-config
Address of remote host [255.255.255.255]? 172.16.101.101
Name of configuration file[rtr2-confg]? host2-confg
Configure using host2-confg from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-confg:![OK]
[OK]
bridge#
%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 15-13.
Step 2		Log into the WMIC 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** *username*	(Optional) Change the default remote username.
Step 5	**ip ftp password** *password*	(Optional) Change the default password.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**copy system:running-config ftp:**[[[**//**[*username*[**:***password*]**@**]*location*]**/***directory*] **/***filename*] or **copy nvram:startup-config ftp:**[[[**//**[*username*[**:***password*]**@**]*location*]**/***directory*] **/***filename*]	Using FTP, store the WMIC 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:

```
bridge# 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
bridge#
```

This example shows how to store a startup configuration file on a server by using FTP to copy the file:

```
bridge# configure terminal
bridge(config)# ip ftp username netadmin2
bridge(config)# ip ftp password mypass
bridge(config)# end
bridge# 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 WMIC. 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 WMIC 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 WMIC software sends the Telnet username as the remote username.
- The WMIC 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 15-16
- Downloading a Configuration File by Using RCP, page 15-16
- Uploading a Configuration File by Using RCP, page 15-17

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 WMIC has a route to the RCP server. The WMIC 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 WMIC 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 WMIC 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 WMIC. 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 WMIC contains these configuration lines:

  ```
  hostname ap1
  ip rcmd remote-username User0
  ```

  If the WMIC 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 15-16.
Step 2		Log into the WMIC 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** *username*	(Optional) Specify the remote username.

	Command	Purpose
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**copy rcp:**[[[//[*username*@]*location*]/*directory*]/*filename*] **system:running-config** or **copy rcp:**[[[//[*username*@]*location*]/*directory*]/*filename*] **nvram: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-confg* 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 WMIC:

```
bridge# copy rcp://netadmin1@172.16.101.101/host1-confg system:running-config
Configure using host1-confg from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-confg:![OK]
bridge#
%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-confg* from the *netadmin1* directory on the remote server with an IP address of 172.16.101.101 to the startup configuration:

```
bridge# configure terminal
bridge(config)# ip rcmd remote-username netadmin1
bridge(config)# end
bridge# copy rcp: nvram:startup-config
Address of remote host [255.255.255.255]? 172.16.101.101
Name of configuration file[rtr2-confg]? host2-confg
Configure using host2-confg from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-confg:![OK]
[OK]
bridge#
%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 15-16.
Step 2		Log into the WMIC 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** *username*	(Optional) Specify the remote username.

	Command	Purpose
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 WMIC 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:

```
bridge# 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
bridge#
```

This example shows how to store a startup configuration file on a server:

```
bridge# configure terminal
bridge(config)# ip rcmd remote-username netadmin2
bridge(config)# end
bridge# 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 WMIC prompts for confirmation on destructive file operations. For more information about the **file prompt** command, refer to the *Cisco IOS Command Reference for Release 12.1*.

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 WMIC image file from a TFTP, FTP, or RCP server to upgrade the WMIC software. You upload an WMIC image file to a TFTP, FTP, or RCP server for backup purposes. You can use this uploaded image for future downloads to the same WMIC 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 WMIC, page 15-19
- tar File Format of Images on a Server or Cisco.com, page 15-19
- Copying Image Files by Using TFTP, page 15-20
- Copying Image Files by Using FTP, page 15-23
- Copying Image Files by Using RCP, page 15-27
- Reloading the Image Using the Web Browser Interface, page 15-32

Note For a list of software images and supported upgrade paths, refer to the release notes for your WMIC.

Image Location on the WMIC

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 WMIC. 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 WMIC
- 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 WMIC image from a TFTP server or upload the image from the WMIC to a TFTP server.

You download an WMIC image file from a server to upgrade the WMIC software. You can overwrite the current image with the new one.

You upload an WMIC image file to a server for backup purposes; this uploaded image can be used for future downloads to the same or another device of the same type.

This section includes this information:

- Preparing to Download or Upload an Image File by Using TFTP, page 15-20
- Downloading an Image File by Using TFTP, page 15-21
- Uploading an Image File by Using TFTP, page 15-22

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 WMIC has a route to the TFTP server. The WMIC 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 15-20
Step 2		Log into the WMIC through a Telnet session.
Step 3	**archive download-sw /overwrite /reload tftp:**[[//*location*]/*directory*]/*image-name*	Download the image file from the TFTP server to the WMIC, 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 *location*, specify the IP address of the TFTP server. • For *directory*/*image-name*, 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 WMIC, 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 *location*, specify the IP address of the TFTP server. • For *directory*/*image-name*, 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 WMIC 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 WMIC to a TFTP server. You can later download this image to the WMIC or to another WMIC 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 15-20.
Step 1		Log into the WMIC through a Telnet session.
Step 2	**archive upload-sw tftp:**[[**//***location*]**/***directory*]**/***image-name***.tar**	Upload the currently running WMIC image to the TFTP server. • For *location*, specify the IP address of the TFTP server. • For *directory***/***image-name***.tar**, specify the directory (optional) and the name of the software image to be uploaded. Directory and image names are case sensitive. The *image-name***.tar** 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 a WMIC image from an FTP server or upload the image from the WMIC to an FTP server.

You download a WMIC image file from a server to upgrade the WMIC software. You can overwrite the current image with the new one or keep the current image after a download.

You upload an WMIC image file to a server for backup purposes. You can use this uploaded image for future downloads to the WMIC or another device of the same type.

This section includes this information:

Preparing to Download or Upload an Image File by Using FTP

You can copy images 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 WMIC 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 WMIC 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 WMIC forms a password named *username@apname.domain*. The variable *username* is the username associated with the current session, ap*name* is the configured host name, and *domain* is the domain of the WMIC.

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 WMIC has a route to the FTP server. The WMIC 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 WMIC 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 WMIC 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 WMIC.

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 15-23.
Step 2		Log into the WMIC 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** *username*	(Optional) Change the default remote username.
Step 5	**ip ftp password** *password*	(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 WMIC, 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 15-23. • 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 WMIC, 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 15-23. • 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 WMIC 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 WMIC to an FTP server. You can later download this image to the same WMIC or to another WMIC 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 15-13.
Step 2		Log into the WMIC 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** *username*	(Optional) Change the default remote username.
Step 5	**ip ftp password** *password*	(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 WMIC image to the FTP server. • 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 15-23. • For **@***location*, specify the IP address of the FTP server. • For **/***directory***/***image-name***.tar**, specify the directory (optional) and the name of the software image to be uploaded. Directory and image names are case sensitive. The *image-name***.tar** 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 a WMIC image from an RCP server or upload the image from the WMIC to an RCP server.

You download a WMIC image file from a server to upgrade the WMIC software. You can overwrite the current image with the new one or keep the current image after a download.

You upload a WMIC image file to a server for backup purposes. You can use this uploaded image for future downloads to the same WMIC or another device of the same type.

This section includes this information:

- Preparing to Download or Upload an Image File by Using RCP, page 15-27
- Downloading an Image File by Using RCP, page 15-29
- Uploading an Image File by Using RCP, page 15-31

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 WMIC. 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 WMIC 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 WMIC software sends the Telnet username as the remote username.
- The WMIC 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 WMIC has a route to the RCP server. The WMIC 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 WMIC 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 WMIC 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 WMIC. For UNIX systems, you must add an entry to the .rhosts file for the remote user on the RCP server. For example, suppose the WMIC contains these configuration lines:

  ```
  hostname ap1
  ip rcmd remote-username User0
  ```

  If the WMIC 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 15-27.
Step 2		Log into the WMIC 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** *username*	(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 WMIC, 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*, 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 15-27. • For @*location*, specify the IP address of the RCP server. • For **/***directory***/***image-name***.tar**, 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 WMIC, 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*, 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 15-27. • For @*location*, specify the IP address of the RCP 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 WMIC 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 an 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 WMIC to an RCP server. You can later download this image to the same WMIC or to another WMIC 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 15-27.
Step 2		Log into the WMIC 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** *username*	(Optional) Specify the remote username.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**archive upload-sw rcp:**[[**//**[*username*@]*location*]**/***directory*]**/***image-name***.tar**]	Upload the currently running WMIC image to the RCP server. • For **//***username*, 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 15-27. • For @*location*, specify the IP address of the RCP server. • For **/***directory*]**/***image-name***.tar**, specify the directory (optional) and the name of the software image to be uploaded. Directory and image names are case sensitive. • The *image-name***.tar** 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 WMIC image file. The Web browser interface supports loading the image file using HTTP or TFTP interfaces.

Note Your WMIC 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 WMIC image file on your PC and download the image to the WMIC. 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 WMIC'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 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 **Upgrade** 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 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 WMIC'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 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 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 **Upgrade** button.

For additional information click the Help icon on the Software Upgrade screen.

Configuring System Message Logging

This chapter describes how to configure system message logging on your WMIC.

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 12.2*.

This chapter consists of these sections:

Understanding System Message Logging

By default, devices 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 command-line interface (CLI) or by saving them to a properly configured syslog server. The device saves syslog messages in an internal buffer. You can remotely monitor system messages by accessing the WMIC 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

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 16-1 describes the elements of syslog messages.

Table 16-1 System Log Message Elements

Element	Description
seq no:	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 16-6.
timestamp formats: *mm/dd hh:mm:ss* or *hh:mm:ss* (short uptime) or *d h* (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 16-6.
facility	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.
severity	Single-digit code from 0 to 7 that is the severity of the message. For a description of the severity levels, see Table 16-3 on page 16-8.
MNEMONIC	Text string that uniquely describes the message.
description	Text string containing detailed information about the event being reported.

This example shows a partial system message:

```
Syslog logging: enabled (0 messages dropped, 3 messages rate-limited, 0 flushes,
 0 overruns, xml disabled)
    Console logging: level debugging, 74 messages logged, xml disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled
    Buffer logging: level debugging, 76 messages logged, xml disabled
    Logging Exception size (4096 bytes)
    Count and timestamp logging messages: disabled
    Trap logging: level informational, 78 message lines logged
Log Buffer (4096 bytes):
CHANGED: Interface Dot11Radio0, changed state to reset
*Mar  1 17:02:19.618: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Mar  1 17:14:21.520: %SYS-5-CONFIG_I: Configured from console by Cisco on vty0
(10.0.0.42)
*Mar  1 17:36:33.519: %SYS-5-CONFIG_I: Configured from console by Cisco on vty0
(10.0.0.42)
*Mar  1 17:56:48.596: %SYS-5-CONFIG_I: Configured from console by Cisco on vty0
(10.0.0.42)
*Mar  1 18:12:01.670: %SYS-5-CONFIG_I: Configured from console by Cisco on vty0
(10.0.0.42)
*Mar  1 19:35:39.710: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to r
eset
*Mar  1 19:35:39.718: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Mar  1 20:52:06.007: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to do
wn
*Mar  1 20:52:06.022: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to r
eset
*Mar  1 20:52:06.035: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Mar  1 23:47:38.851: %DOT11-6-ASSOC: Interface Dot11Radio0, Station  0002.8a29.
```

```
82e8 Associated KEY_MGMT[NONE]
*Mar  1 23:48:16.986: %DOT11-6-DISASSOC: Interface Dot11Radio0, Deauthenticating
 Station 0002.8a29.82e8 Reason: Previous authentication no longer valid
```

Default System Message Logging Configuration

Table 16-2 shows the default system message logging configuration.

Table 16-2 Default System Message Logging Configuration

Feature	Default Setting
System message logging to the console	Enabled
Console severity	Debugging (and numerically lower levels; see Table 16-3 on page 16-8)
Logging buffer size	4096 bytes
Logging history size	1 message
Timestamps	Disabled
Synchronous logging	Disabled
Logging server	Disabled
Syslog server IP address	None configured
Server facility	Local7 (see Table 16-4 on page 16-11)
Server severity	Informational (and numerically lower levels; see Table 16-3 on page 16-8)

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 WMIC 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 16-6.

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** [*size*] [*level*]	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 WMIC could run out of memory for other tasks. Use the **show memory** privileged EXEC command to view the free processor memory on the WMIC; however, this value is the maximum available, and you should *not* set the buffer size to this amount.
Step 3	**logging** *host*	Log messages to a UNIX syslog server host. For *host*, 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 16-10.
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 s**ervice 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 16-3.

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** *level*	Limit messages logged to the console. By default, the console receives debugging messages and numerically lower levels (see Table 16-3 on page 16-8).
Step 3	**logging monitor** *level*	Limit messages logged to the terminal lines. By default, the terminal receives debugging messages and numerically lower levels (see Table 16-3 on page 16-8).
Step 4	**logging trap** *level*	Limit messages logged to the syslog servers. By default, syslog servers receive informational messages and numerically lower levels (see Table 16-3 on page 16-8). For complete syslog server configuration steps, see the "Configuring UNIX Syslog Servers" section on page 16-10.
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 16-3 describes the *level* keywords. It also lists the corresponding UNIX syslog definitions from the most severe level to the least severe level.

Table 16-3 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 WMIC 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; WMIC functionality is not affected.
- Reload requests and low-process stack messages, displayed at the **informational** level. This message is only for information; WMIC 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 WMIChistory 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 16-3 on page 16-8) 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** *level*[1]	Change the default level of syslog messages stored in the history file and sent to the SNMP server. See Table 16-3 on page 16-8 for a list of *level* keywords. By default, **warnings**, **errors**, **critical**, **alerts**, and **emergencies** messages are sent.
Step 3	**logging history size** *number*	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 16-3 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 device 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** *seconds* [**all** | **console**] [**except** *severity*]	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/logs/cisco.log
```

The **local7** keyword specifies the logging facility to be used; see Table 16-4 on page 16-11 for information on the facilities. The **debug** keyword specifies the syslog level; see Table 16-3 on page 16-8 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 WMIC 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** *level*	Limit messages logged to the syslog servers. Be default, syslog servers receive informational messages and lower. See Table 16-3 on page 16-8 for *level* keywords.
Step 4	**logging facility** *facility-type*	Configure the syslog facility. See Table 16-4 on page 16-11 for *facility-type* 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 16-4 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 16-4 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 12.2*.

To display the logging history file, use the **show logging history** privileged EXEC command.

Wireless Device Troubleshooting

This chapter provides troubleshooting procedures for basic problems with the wireless device. For the most up-to-date, detailed troubleshooting information, refer to the Cisco TAC website at the following URL (select **Top Issues** and then select **Wireless Technologies**):

http://www.cisco.com/tac

Sections in this chapter include:

Checking the LED Indicators

If your wireless device is not communicating, check theLED indicatorsto quickly assess the device status.

The indicator signals on the wireless device have the following meanings (for additional details refer to Table 17-1):

- The Ethernet indicator signals traffic on the wired LAN. This indicator is normally green when an Ethernet cable is connected, and blinks green when a packet is received or transmitted over the Ethernet infrastructure. The indicator is off when the Ethernet cable is not connected.
- The status indicator signals operational status. Steady green indicates that the wireless device is associated with at least one wireless client. Blinking green indicates that the wireless device is operating normally but is not associated with any wireless devices.
- The radio indicator blinks green to indicate radio traffic activity. The light is normally off, but it blinks whenever a packet is received or transmitted over the wireless device radio.

Table 17-1 Indicator Signals

Message type	Ethernet indicator	Status indicator	Radio indicator	Meaning
Boot loader status	Green	–	Green	DRAM memory test.
	–	Amber	Red	Board initialization test.
	–	Blinking green	Blinking green	Flash memory test.
	Amber	Green	–	Ethernet initialization test.
	Green	Green	Green	Starting Cisco IOS software.
Association status	–	Green	–	At least one wireless client device is associated with the unit.
	–	Blinking green	–	No client devices are associated; check the wireless device SSID and WEP settings.
Operating status	–	Green	Blinking green	Transmitting/receiving radio packets.
	Green	–	–	Ethernet link is operational.
	Blinking green	–	–	Transmitting/receiving Ethernet packets.
Boot Loader Errors	Red	–	Red	DRAM memory test failure.
	–	Red	Red	File system failure.
	Red	Red	–	Ethernet failure during image recovery.
	Amber	Green	Amber	Boot environment error.
	Red	Green	Red	No Cisco IOS image file.
	Amber	Amber	Amber	Boot failure.

Table 17-1 Indicator Signals (continued)

Message type	Ethernet indicator	Status indicator	Radio indicator	Meaning
Operation Errors	–	Green	Blinking amber	Maximum retries or buffer full occurred on the radio.
	Blinking amber	–	–	Transmit/receive Ethernet errors.
	–	Blinking amber	–	General warning.
Configuration Reset	–	Amber	–	Resetting the configuration options to factory defaults.
Failures	Red	Red	Red	Firmware failure; try disconnecting and reconnecting unit power.
	Blinking red	–	–	Hardware failure. The wireless device must be replaced.
Firmware Upgrade	–	Red	–	Loading new firmware image.

Checking Basic Settings

Mismatched basic settings are the most common causes of lost connectivity with wireless clients. If the wireless device does not communicate with client devices, check the areas described in this section.

SSID

Wireless clients attempting to associate with the wireless device must use the same SSID as the wireless device. If a client device SSID does not match the SSID of an wireless device in radio range, the client device will not associate. The wireless device default SSID is *tsunami*.

WEP Keys

The WEP key you use to transmit data must be set up exactly the same on the wireless device 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 wireless device to exactly the same value. The wireless device does not need to use Key 3 as its transmit key, however.

Security Settings

Wireless clients attempting to authenticate with the wireless device must support the same security options configured in the wireless device, 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 wireless device, 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 wireless device settings.

Note The wireless device MAC address that appears on the Status page in the Aironet Client Utility (ACU) is the MAC address for the wireless device radio.

Resetting to the Default Configuration

If you forget the password that allows you to configure the wireless device, you may need to completely reset the 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 these steps to delete the current configuration and return all wireless device settings to the factory defaults using the web browser 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 wireless device 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 wireless device password 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 the **Reset to Defaults** button.

Note If the wireless device is configured with a static IP address, the IP address does not change.

Step 8 After the wireless device reboots, you must reconfigure the wireless device by using the Web-browser interface or the CLI. The default username and password are **Cisco**, which is case-sensitive.

Using the CLI

Follow the steps below to delete the current configuration and return all wireless device settings to the factory defaults using the CLI.

Step 1 Open the CLI using a Telnet session or a connection to the wireless device console port.

Step 2 Reboot the wireless device by removing power from and reapplying power to the router.

Step 3 Let the wireless device boot until the command prompt appears and the wireless device begins to inflate the image. When you see these lines on the CLI, press **Esc**:

```
Loading "flash:/c350-k9w7-mx.v122_13_ja.20031010/c350-k9w7-mx.v122_13_ja.20031010"
...###########################################################################
################################################################################
################################################################################
####################
```

Step 4 At the ap: prompt, enter the **flash_init** command to initialize the Flash.

```
ap: flash_init
Initializing Flash...
flashfs[0]: 142 files, 6 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 7612416
flashfs[0]: Bytes used: 3407360
flashfs[0]: Bytes available: 4205056
flashfs[0]: flashfs fsck took 0 seconds.
...done initializing Flash.
```

Step 5 Use the **dir flash:** command to display the contents of Flash and find the config.txt configuration file.

```
ap: dir flash:
Directory of flash:/
3 .rwx 223 <date> env_vars
4 .rwx 2190 <date> config.txt
5 .rwx 27 <date> private.config
150 drwx 320 <date> c350.k9w7.mx.122.13.JA
4207616 bytes available (3404800 bytes used)
```

Step 6 Use the **rename** command to change the name of the config.txt file to config.old.

```
ap: rename flash:config.txt flash:config.old
```

Step 7 Use the **reset** command to reboot the wireless device.

```
ap: reset
Are you sure you want to reset the system (y/n)?y
System resetting..Xmodem file system is available.
flashfs[0]: 142 files, 6 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 7612416
flashfs[0]: Bytes used: 3407360
flashfs[0]: Bytes available: 4205056
flashfs[0]: flashfs fsck took 0 seconds.
Reading cookie from flash parameter block...done.
Base ethernet MAC Address: 00:40:96:41:e4:df
Loading "flash:/c350.k9w7.mx.122.13.JA/c350.k9w7.mx.122.13.JA"...######## . . .
```

Note The wireless device is configured with factory default values, including the IP address (set to receive an IP address using DHCP) and the default username and password (**Cisco**).

Step 8 When IOS software is loaded, you can use the **del** privileged EXEC command to delete the config.old file from Flash.

```
ap# del flash:config.old
Delete filename [config.old]
Delete flash:config.old [confirm]
ap#
```

Reloading the Image

If the wireless device has a firmware failure, you must reload the image file using the Web browser interface. You can use the browser interface if the wireless device firmware is still fully operational and you want to upgrade the firmware image.

If the wireless device experiences a firmware failure or a corrupt firmware image, indicated by three red LED indicators, you must reload the image from a connected TFTP server.

Note This process resets *all* configuration settings to factory defaults, including passwords, WEP keys, the wireless device IP address, and SSIDs.

Using the Web Browser Interface

You can also use the Web browser interface to reload the wireless device image file. The Web broswer interface supports loading the image file using HTTP or TFTP interfaces.

Note Your wireless device configuration does not change when you use the browser to reload the image file.

Browser HTTP Interface

The HTTP interface enables you to browse to the wireless device image file on your PC and download the image to the wireless device. 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 wireless device 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 wireless device 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 find the image file on your PC.

Step 7 Click **Upload**.

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 wireless device 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 wireless device 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 wireless device 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 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 **Upload**.

For additional information click the **Help** icon on the Software Upgrade screen.

Using the CLI

Follow the steps below to reload the wireless device image using the CLI. When the wireless device begins to boot, interrupt the boot process and use boot loader commands to load an image from a TFTP server to replace the image in the wireless device.

Note Your wireless device 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 wireless device console port.

Step 2 Reboot the wireless device by removing power and reapplying power.

Step 3 Let the wireless device boot until it begins to inflate the image. When you see these lines on the CLI, press **Esc**:

```
Loading "flash:/c350-k9w7-mx.v122_13_ja.20031010/c350-k9w7-mx.v122_13_ja.20031010"
...###########################################################################
################################################################################
################################################################################
####################
```

Step 4 When the ap: command prompt appears, enter the **set** command to assign an IP address, subnet mask, and default gateway to the wireless device.

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 wireless device 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 wireless device Flash)

Your entry might look like this example:

```
ap: tar -xtract tftp://192.168.130.222/images/c350-k9w7-tar.122-13.JA1 flash:
```

Step 7 When the display becomes full, the CLI pauses and displays `--MORE--`. Press the spacebar to continue.

```
extracting info (229 bytes)
c350-k9w7-mx.122-13.JA1/ (directory) 0 (bytes)
c350-k9w7-mx.122-13.JA1/html/ (directory) 0 (bytes)
c350-k9w7-mx.122-13.JA1/html/level1/ (directory) 0 (bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/appsui.js (558 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/back.htm (205 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/cookies.js (5027 bytes).
extracting c350-k9w7-mx.122-13.JA1/html/level1/forms.js (15704 bytes)...
extracting c350-k9w7-mx.122-13.JA1/html/level1/sitewide.js (14621 bytes)...
extracting c350-k9w7-mx.122-13.JA1/html/level1/config.js (2554 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/stylesheet.css (3215 bytes)
c350-k9w7-mx.122-13.JA1/html/level1/images/ (directory) 0 (bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/ap_title_appname.gif (1422 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_button_1st.gif (1171 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_button_cbottom.gif (318 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_button_current.gif (348 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_button_last.gif (386 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_button_last_filler.gif (327
bytes)
```

```
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_button_last_flat.gif (318
bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_button_nth.gif (1177 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_leftnav_dkgreen.gif (869 bytes)
 -- MORE --
```

Note If you do not press the spacebar to continue, the process eventually times out and the wireless device stops inflating the image.

Step 8 Enter the **set BOOT** command to designate the new image as the image that the wireless device uses when it reboots. The wireless device 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:/c350-k9w7-mx.122-13.JA1/c350-k9w7-mx.122-13.JA1
```

Step 9 Enter the **set** command to check your bootloader entries.

```
ap: set
BOOT=flash:/c350-k9w7-mx.122-13.JA1/c350-k9w7-mx.122-13.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 wireless device. When the wireless device reboots, it loads the new image.

```
ap: boot
```

Obtaining the Image File

You can obtain the wireless device image file from the Cisco.com software center by following these steps:

Step 1 Use your Internet browser to access the Cisco Software Center at the following URL:

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

Step 2 Find the wireless device firmware and utilities section and click on the link for the wireless device.

Step 3 Double-click the latest firmware image file for wireless devices.

Step 4 Download the image file to a directory on your PC hard drive.

Obtaining TFTP Server Software

You can download TFTP server software from several websites. 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.

Reloading the Bootloader Image

Follow this procedure to download the boot loader image to the device:

Step 1 Place the bootloader image in the proper directory on a TFTP server.

Step 2 Connect to the console.

Step 3 Enter the **enable** command to enter privileged mode.

Step 4 Download the new boot loader image from the TFTP server to the boot sector by using the **copy tftp://***ip address***/***path***/***imagename* **bs:** command, where ip address is the address of the TFTP server and path is the path to the directory where the boot loader image is located.

> **Caution** The boot sector Flash file system is addressed as **bs:**. The WMIC will not boot up and will not recover if a non-bootloader image is downloaded to the boot sector of the Flash file system.

Step 5 When the boot loader download is complete, enter the **reset** command at the console prompt to reset the device.

Step 6 When the boot loader upgrade is complete, enter the **boot** command at the console prompt to reboot the device.

Step 7 Enter the **version** commmand to verify that it boots using the upgraded boot loader.

Example Command Output

```
bridge: copy tftp://223.255.254.253/tftpboot/jrehage/loader_c3202_bs.img bs:
................................................................
File "tftp://223.255.254.253/tftpboot/jrehage/loader_c3202_bs.img" successfully copied to
"bs:"
bridge:reset
Are you sure you want to reset the system (y/n)?y
System resetting...
                   Xmodem file system is available.
flashfs[0]:136 files, 6 directories
flashfs[0]:0 orphaned files, 0 orphaned directories
flashfs[0]:Total bytes:15998976
flashfs[0]:Bytes used:7458304
flashfs[0]:Bytes available:8540672
flashfs[0]:flashfs fsck took 30 seconds.
Base ethernet MAC Address:00:ff:ff:f0:01:4f
Initializing ethernet port 0...
Reset ethernet port 0...
Reset done!
ethernet link up, 100 mbps, full-duplex
Ethernet port 0 initialized:link is up
```

Connecting to the Cisco 3200 Series Router and Using the Command-Line Interface

This chapter describes how to connect to the router and use the IOS command-line interface (CLI) that you can use to configure the WMIC. It contains these sections:

Before You Start

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

- A system name for the WMIC
- The case-sensitive wireless service set identifier (SSID) that your WMICs use
- If not connected to a DHCP server, a unique IP address for your WMIC (such as 172.17.255.115)
- If the WMIC 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)

Resetting the WMIC to the Default Settings

You can use the CLI to reset the WMIC 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.

From the privileged EXEC mode, you can reset the WMIC 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. You can see the following CLI message when the load process has finished: *Line protocal on Interface Dot11Radio0, changed state to up*.

Step 5 After the WMIC reboots, you can reconfigure the WMIC by using the Web-browser interface or the CLI.

To obtain the WMIC's new IP address, you can use the **show interface bvi1** CLI command.

Assigning an IP Address

To assign the WMIC IP address by using one of the following methods:

- Use the **ip address** interface command to assign an IP address to the interface.
- Use a DHCP server (if available) to automatically assign an IP address.

The WMIC links to the network using a Bridge Group Virtual Interface (BVI) that it creates automatically. Instead of tracking separate IP addresses for the WMIC Ethernet and radio ports, the network uses the BVI.

Note The WMIC supports only one BVI on each WMIC. Configuring more than one BVI might cause errors in the WMIC ARP table.

When you assign an IP address to the WMIC 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 BVI:

	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** *address mask*	Assign an IP address and address mask to the BVI. **Note** If you are connected to the WMIC using a Telnet session, you lose your connection to the WMIC when you assign a new IP address to the BVI. To continue configuring the WMIC using Telnet, use the new IP address to open another Telnet session to the WMIC.

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 WMIC, 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 WMIC 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 WMIC 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 A-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 A-1 Command Mode Summary

Mode	Access Method	Prompt	Exit Method	About This Mode
User EXEC	Begin a session with your WMIC.	`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 device.
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 A-2.

Table A-2 Help Summary

Command	Purpose
help	Obtains a brief description of the help system in any command mode.

*abbreviated-command-entry***?**	Obtains a list of commands that begin with a particular character string.
	For example:
	`bridge# di?`
	`dir  disable  disconnect`

abbreviated-command-entry<**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> ?`
command **?**	Lists the associated keywords for a command. For example: `bridge> show ?`

command keyword **?**	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 WMIC 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 A-3 lists some error messages that you might encounter while using the CLI to configure your WMIC.

Table A-3 Common CLI Error Messages

Error Message	Meaning	How to Get Help
`% Ambiguous command: "show con"`	You did not enter enough characters for your WMIC 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 A-7
- Recalling Commands, page A-7
- Disabling the Command History Feature, page A-7

Changing the Command History Buffer Size

By default, the WMIC 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 WMIC records during the current terminal session:

```
bridge# 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 WMIC records for all sessions on a particular line:

```
bridge(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 A-4:

Table A-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 A-8
- Editing Commands Through Keystrokes, page A-8
- Editing Command Lines that Wrap, page A-9

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:

```
bridge# terminal editing
```

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

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

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

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

Editing Commands Through Keystrokes

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

Table A-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 WMIC 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.

Table A-5 Editing Commands Through Keystrokes (continued)

Capability	Keystroke[1]	Purpose
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.
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 `More` 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 `More` prompt.	**Return**	Scroll down one line.
	Space	Scroll down one screen.
Redisplay the current command line if the WMIC 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.

```
bridge(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1
bridge(config)# $ 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.25
bridge(config)# $t tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq
bridge(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:

```
bridge(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 A-8.

Searching and Filtering the 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:

```
bridge# 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
```

Channels and Antenna Settings

This appendix lists the IEEE 802.11g (2.4-GHz) channels, maximum power levels, and antenna gains supported by the world's regulatory domains.

The following topics are covered in this appendix:

- Channels, page B-2
- Maximum Power Levels and Antenna Gains, page B-4

See the "Configuring Radio Transmit Power" in the "Configuring Radio Settings" chapter for instructions about how to change the radio output power.

Channels

This section describes the channels for 802.11b/g (2.4-GHz) and the 4.9-GHz bands.

IEEE 802.11g (2.4-GHz Band)

The channel identifiers, channel center frequencies, and regulatory domains of each IEEE 802.11g 22-MHz-wide channel are shown in Table B-1.

Table B-1 Channels for IEEE 802.11g

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
10	2457	X	X	X	X	–	–	X	X
11	2462	X	X	X	X	–	–	X	X
12	2467	–	–	X	X	–	–	X	X
13	2472	–	–	X	X	–	–	X	X
14	2484	–	–	–	–	–	–	X	–

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

4.9-GHz Band

The channel identifiers, channel center frequencies, and channel width are shown in Table B-2.

Table B-2 Channels, Center Frequencies, and Channel Widths

Channel	Center Frequency	Channel Width
1	4940.5	not supported
2	4941.5	not supported
3	4942.5	5-MHz
4	4943.5	not supported
5	4944.5	not supported
6	4947.5	5-MHz
7	4952.5	5-MHz, 10-MHz, or 20-MHz
8	4957.5	5-MHz
9	4962.5	5-MHz or 10-MHz
10	4967.5	5-MHz
11	4972.5	5-MHz, 10-MHz, or 20-MHz
12	4977.5	5-MHz
13	4982.5	5-MHz or 10-MHz
14	4985.5	not supported
15	4986.5	5-MHz
16	4987.5	not supported
17	4988.5	not supported
18	4989.5	not supported

Maximum Power Levels and Antenna Gains

IEEE 802.11g (2.4-GHz Band)

An improper combination of power level and antenna gain can result in equivalent isotropic radiated power (EIRP) above the amount allowed per regulatory domain. Table B-3 indicates the maximum power levels and antenna gains allowed for each IEEE 802.11g regulatory domain.

Note To meet regulatory restrictions, the external antenna BR1300 configuration 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.

Table B-3 Maximum Power Levels Per Antenna Gain for IEEE 802.11g

Regulatory Domain	Antenna Gain (dBi)	Maximum Power Level (mW)	
		CCK	**OFDM**
Americas (–A) (4 W EIRP maximum)	2.2	100	30
	6	100	30
	6.5	100	30
	10	100	30
	13.5	100	30
	15	50	20
	21	20	10
EMEA (–E) and Israel(-I) (100 mW EIRP maximum)	2.2	50	30
	6	30	10
	6.5	20	10
	10	10	5
	13.5	5	5
	15	5	1
	21	1	—
Japan (-J) (10 mW/MHz EIRP maximum)	2.2	5	5
	6	5	5
	6.5	5	5
	10	5	5
	13.5	5	5
	15	5	5
	21	5	5

Protocol Filters

The tables in this appendix list some of the protocols that you can filter on the WMIC. The tables include:

- Table E-1, Ethertype 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 C-1 Ethertype Protocols

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

Table C-2 IP Protocols

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

Table C-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 quote	17
Message Send Protocol	msp	18
ttytst source	chargen	19
FTP Data	ftp-data	20
FTP Control (21)	ftp	21
Secure Shell (22)	ssh	22
Telnet	—	23
Simple Mail Transport Protocol	SMTP mail	25
time	timserver	37
Resource Location Protocol	RLP	39
IEN 116 Name Server	name	42
whois	nicname 43	43
Domain Name Server	DNS domain	53
MTP	—	57
BOOTP Server	—	67
BOOTP Client	—	68
TFTP	—	69
gopher	—	70
rje	netrjs	77
finger	—	79
Hypertext Transport Protocol	HTTP www	80
ttylink	link	87
Kerberos v5	Kerberos krb5	88
supdup	—	95
hostname	hostnames	101

Table C-3 IP Port Protocols (continued)

Protocol	Additional Identifier	ISO Designator
TSAP	iso-tsap	102
CSO Name Server	cso-ns csnet-ns	105
Remote Telnet	rtelnet	107
Postoffice v2	POP2 POP v2	109
Postoffice v3	POP3 POP v3	110
Sun RPC	sunrpc	111
tap ident authentication	auth	113
sftp	—	115
uucp-path	—	117
Network News Transfer Protocol	Network News readnews nntp	119
USENET News Transfer Protocol	Network News readnews nntp	119
Network Time Protocol	ntp	123
NETBIOS Name Service	netbios-ns	137
NETBIOS Datagram Service	netbios-dgm	138
NETBIOS Session Service	netbios-ssn	139
Interim Mail Access Protocol v2	Interim Mail Access Protocol IMAP2	143
Simple Network Management Protocol	SNMP	161
SNMP Traps	snmp-trap	162
ISO CMIP Management Over IP	CMIP Management Over IP cmip-man CMOT	163
ISO CMIP Agent Over IP	cmip-agent	164
X Display Manager Control Protocol	xdmcp	177
NeXTStep Window Server	NeXTStep	178
Border Gateway Protocol	BGP	179
Prospero	—	191
Internet Relay Chap	IRC	194

Table C-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 uucpd	540
Kerberos rlogin	klogin	543
Kerberos rsh	kshell	544
rfs_server	remotefs	556
Kerberos kadmin	kerberos-adm	749
network dictionary	webster	765
SUP server	supfilesrv	871
swat for SAMBA	swat	901
SUP debugging	supfiledbg	1127
ingreslock	—	1524
Prospero non-priveleged	prospero-np	1525
RADIUS	—	1812
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 WMIC supports. The Cisco IOS SNMP agent supports both SNMPv1 and SNMPv2. This appendix contains these sections:

- MIB List, page D-1
- Using FTP to Access the MIB Files, page D-2

MIB List

- BRIDGE-MIB
- CISCO-AAA-SERVER-MIB
- CISCO-CDP-MIB
- CISCO-CLASS-BASED-QOS-MIB
- CISCO-CONFIG-COPY-MIB
- CISCO-CONFIG-MAN-MIB
- CISCO-DOT11-ASSOCIATION-MIB
- CISCO-DOT11-IF-MIB
- CISCO-ENTITY-VENDORTYPE-OID-MIB
- CISCO-ENV-MON-MIB
- CISCO-FLASH-MIB
- CISCO-IETF-DOT11-QOS-MIB
- CISCO-IETF-DOT11-QOS-EXT-MIB
- CISCO-IMAGE-MIB
- CISCO-IP-PROTOCOL-FILTER-MIB
- CISCO-MEMORY-POOL-MIB
- CISCO-PROCESS-MIB
- CISCO-PRODUCTS-MIB
- CISCO-SMI
- CISCO-SYSLOG-MIB

- CISCO-SYSLOG-EVENT-EXT-MIB
- CISCO-TC
- CISCO-TBRIDGE-DEV-IF-MIB
- CISCO-WLAN-VLAN-MIB
- ENTITY-MIB
- IANAifType-MIB
- IEEE802dot11-MIB
- IF-MIB
- INET-ADDRESS-MIB
- OLD-CISCO-SYS-MIB
- OLD-CISCO-SYSTEM-MIB
- OLD-CISCO-TS-MIB
- P-BRIDGE-MIB
- Q-BRIDGE-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

APPENDIX E

Error and Event Messages

This appendix lists the CLI error and event messages. Table E-1 lists the errors and events and provides an explanation and recommended action for each message.

Table E-1 Error and Event Messages

Message	Explanation	Recommended Action
Software Auto Upgrade Messages		
SW_AUTO_UPGRADE-FATAL: Attempt to upgrade software failed, software on Flash may be deleted. Please copy software into Flash.	Auto upgrade of the software failed. The software on the Flash memory might have been deleted. Copy software into the Flash memory.	Copy software before rebooting the unit.
SW_AUTO_UPGRADE-7-FAILURE: dhcp_client_start_stop failed	Auto upgrade of the software failed due to error in starting/stopping DHCP client process.	Copy the error message exactly as it appears and report it to your technical support representative.
SW_AUTO_UPGRADE-7-FAILURE: Failed to obtain ip addr from dhcp server	Auto upgrade of the software failed.	Copy the error message exactly as it appears and report it to your technical support representative.
SW_AUTO_UPGRADE-7-FAILURE: boot_file_pathent creation failed	Auto upgrade of the software failed due to error in creation of pathent (internal data structure).	Copy the error message exactly as it appears and report it to your technical support representative.
Association Management Messages		
DOT11-2-RADIO_HW_RESET: Radio subsystem is under going hardware reset to recover from problem	Radio must be reset due to problem.	None.
DOT11-3-BADSTATE: [mac-address] [chars] [chars] -> [chars]	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.	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.
DOT11-3-RADIO_OVER_ TEMPERATURE: Interface [interface] Radio over temperature	The WMIC detected that the unit has exceeded the radio operating temperature.	Investigate and take steps to cool the unit.

Table E-1 Error and Event Messages (continued)

Message	Explanation	Recommended Action
DOT11-3-RADIO_IF_LO: Interface [interface] Radio cannot lock IF freq	The unit cannot lock the intermediate frequency.	None.
DOT11-3-RADIO_RF_LO: Interface [interface] Radio cannot lock RF freq	The unit cannot lock the radio frequency.	None.
DOT11-3-RF_LOOPBACK_FAILURE: Interface [interface] Radio failed to pass RF loopback test	Radio loopback test failed at startup time.	None.
DOT11-3-TX_PWR_OUT_OF_ RANGE: Interface [interface] Radio Tx power control out of range	The unit has detected that the radio transmit power cannot be locked within the operating range.	None.
DOT11-4-MAXERTRIES: Packet to client [mac] reached max retries, remove the client	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.	None.
DOT11-6-ASSOC: Interface [interface], Station [char] [mac] Associated	A station associated to a bridge.	None.
DOT11-6-ADD: Interface [interface], Station [mac] Associated to Parent [mac]	A station associated to a bridge.	None.
DOT11-6-DISASSOC: Interface [interface], Deauthenticating Station [mac] [char]	A station disassociated from a bridge.	None.
DOT11-6-ROAMED: Station [mac-address] Roamed to [mac-address]	A station has roamed to a new bridge.	None.
Unzip Messages		
SOAP-4-UNZIP_OVERFLOW: Failed to unzip Flash:/c1200-k9w7-mx.122-3.6.JA1/html/level15/ap_xxx.htm.gz, exceeds maximum uncompressed html size	The HTTP server cannot retrieve a compressed file in response to an HTTP GET request because the size of the file is too large for the buffers used in the uncompression process.	Make sure file is a valid HTML page. If so, you'll have to copy an uncompressed version of the file into Flash to retrieve it through HTTP.
802.11 Subsystem Messages		
DOT11-6-FREQ_INUSE: Radio frequency [int] is in use	When scanning for an unused frequency, the unit recognized another radio using the displayed frequency.	None.
DOT11-6-FREQ_USED: Radio frequency [int] selected	After scanning for an unused frequency, the unit selected the displayed frequency.	None.
DOT11-4-VERSION_MISMATCH: Require radio version [hex].[int], found version [hex].[int]	When starting the radio, the wrong firmware version was found. The radio will be loaded with the required version.	None.
DOT11-2-VERSION_INVALID: Unable to find required radio version [hex].[int]	When trying to re-flash the radio firmware, the device recognized that the radio firmware packaged with the IOS firmware had the incorrect version.	None.

Table E-1 Error and Event Messages (continued)

Message	Explanation	Recommended Action
DOT11-4-NO_SSID: No SSIDs configured, radio not started	All SSIDs were deleted from the configuration. At least one must be configured for the radio to run.	Configure at least one SSID on the device.
DOT11-4-FLASHING_RADIO: Flashing the radio firmware ([chars])	The radio has been stopped to load new firmware.	None.
DOT11-2-NO_FIRMWARE: No radio firmware file ([chars]) was found	When trying to Flash new firmware into the radio, the file for the radio was not found in the Flash file system.	The wrong image has been loaded into the unit. Locate the correct image based on the type of radio used.
DOT11-2-BAD_FIRMWARE: Radio firmware file ([chars]) is invalid	When trying to Flash new firmware into the radio, the file was found to be invalid.	Put the correct firmware image file in the place where the unit is looking.
DOT11-4-FLASH_RADIO_DONE: Flashing the radio firmware completed	The radio firmware Flash is complete, and the radio will be restarted with the new firmware.	None.
DOT11-4-LINK_DOWN: Radio parent lost: [chars]	The connection to the parent bridge was lost for the displayed reason. The unit will try to find a new parent bridge.	None.
DOT11-4-CANT_ASSOC: Cannot associate: [chars]	The unit could not establish a connection to a parent bridge for the displayed reason.	Check the configuration of both the parent bridge and this unit to make sure the basic settings (SSID, WEP, and others) match.
Inter-Bridge Protocol Messages		
DOT11-6-ROAMED: Station [mac-address] Roamed to [mac-address]	A station has roamed to a new bridge.	None.
DOT11-6-STANDBY_ACTIVE: Standby to Active, Reason = [chars] ([int])	The device is transitioning from standby mode to active mode.	None.
DOT11-6-ROGUE_AP: Rogue AP [mac-address] reported. Reason: [chars]	A station has reported a potential rogue bridge for the stated reason.	None.
SCHED-3-UNEXPECTEDMESSAGE: Unknown message [hex] received (ptr arg [hex], num arg [hex]).	A process can register to be notified when various events occur in the router. This message indicates that a process received a message from another process that it does not know how to handle.	Copy the error message exactly as it appears, and report it to your technical support representative.
SCHED-3-UNEXPECTEDEVENT: Process received unknown event (maj [hex], min [hex]).	A process can register to be notified when various events occur in the router. This message indicates that a process received an event that it did not know how to handle.	Copy the error message exactly as it appears, and report it to your technical support representative.
Miscellaneous Messages		

Table E-1 Error and Event Messages (continued)

Message	Explanation	Recommended Action
WGB_CLIENT_VLAN: Workgroup Bridge Ethernet client VLAN not configured.	A VLAN configuration is missing for client devices connected to a workgroup bridge.	Use the workgroup-bridge client-vlan command to assign a VLAN to Ethernet client devices connected to the workgroup bridge.
UNDER_VOLTAGE: Under voltage condition detected.	The hardware under voltage detection logic has reported a low voltage condition.	Check the power supply and associated power connections.

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.

802.11a The IEEE standard that specifies carrier sense media access control and physical layer specifications for wireless LANs operating in the 5-GHz frequency 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.

A

access point A wireless LAN data transceiver that uses radio waves to connect a wired network with wireless stations.

AC_BE Access Category Best Effort

AC_BK Access Category Background

AC_VI Access Category Video

AC_VO Access Category Voice

AES Counter-Mode/CBC-MAC protocol (AES CCMP) A protocol based on AES using the CCM mode of operation. The CCM mode combines *Counter* (CTR) mode privacy and *Cipher Block Chaining Message Authentication Code* (CBC-MAC) authentication

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.

authentication suite A suggested set of authentication methods

B

backoff time The random length of time that a station waits before sending a packet on the LAN. Backoff time is a multiple of slot time, so a decrease in slot time ultimately decreases the backoff time, which increases throughput.

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.

BPDU 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.

BPSK A modulation technique used by IEEE 802.11b-compliant wireless LANs for transmission at 1 Mbps.

broadcast packet A single data message (packet) sent to all addresses on the same subnet.

C

CCK Complementary code keying. A modulation technique used by IEEE 802.11b-compliant wireless LANs for transmission at 5.5 and 11 Mbps.

CCKM 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.

cell 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.

client A radio device that uses the services of an Access Point to communicate wirelessly with other devices on a local area network.

Cipher Suite A set of one or more cryptographic algorithms designed to protect data traffic. A cipher suite may provide data privacy, data authenticity or integrity, and/or replay protection

Cisco Centralized Key Management (CCKM) CCKM is the basis of Cisco Fast reassociation and reauthentication solution, which utilizes a central node, an AP, as the key distributor to enable protected communications between the AP and the Wireless Stations. Station using CCKM use proprietary supports SSN Group Key update.

CKIP Cisco Temporal Key Integrity Protocol

client A radio device that uses the services of an access point to communicate wirelessly with other devices on a local area network.

CMIC Cisco Message Integrity Check

CSMA Carrier sense multiple access. A wireless LAN media access method specified by the IEEE 802.11 specification.

D

data rates The range of data transmission rates supported by a device. Data rates are measured in megabits per second (Mbps).

dBi 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.

DHCP 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.

dipole A type of low-gain (2.2-dBi) antenna consisting of two (often internal) elements.

domain name 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.

DNS 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.

DSSS Direct sequence spread spectrum. A type of spread spectrum radio transmission that spreads its signal continuously over a wide frequency band.

E

EAP 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.

EAPOL-Key Key Combination of EAPOL-Key Encryption key and EAPOL-Key MIC Key.

EAPOL Key Encryption Key (KEK) Key that encrypts key material in EAPOL-key packet

EAPOL-Key MIC Key (KCK) Key used to integrity check an EAPOL-Key Message.

Ethernet 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

file server A repository for files so that a local area network can share files, mail, and programs.

firmware Software that is programmed on a memory chip.

G

gateway A device that connects two otherwise incompatible networks.

GHz Gigahertz. One billion cycles per second. A unit of measure for frequency.

I

IEEE 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.

infrastructure The wired Ethernet network.

IP address 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.

Message Integrity Code (MIC) A cryptographic checksum, designed to make it computationally infeasible for an adversary to alter data. This is usually called a Message Authentication Code, or MAC, in the literature, but the acronym MAC is already reserved for another meaning in this standard.

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.

pairwise Two entities that is associated with each other; an access point and one associated station, or a pair of stations in an IBSS network, used to describe the key hierarchies for keys that are shared only between the two entities in a pairwise.

Pairwise Master Key (PMK) The key that is generated on a per-session basis and is used as one of the inputs into the PRF to derive the Pairwise Transient Keys (PTK). For EAP-TLS authentication, the Pairwise Master Key is the key from the RADIUS MS-MPPE-Recv-Key attribute. For Pre-Shared Key authentication, the Pairwise Master Key is the Pre-Shared Key.

PMKID PMK identification

Pairwise Transient Key (PTK) A value that is derived from the PRF using the SNonce and ANonce, and is split up into as many as five keys (Temporal Encryption Key, two Temporal MIC Keys, EAPOL-Key Encryption Key, EAPOL-Key MIC Key) for use by the rest of the system.

Pre-Shared Key (PSK) A key that is distributed to the units in the system by manual means. Legacy WEP systems without authentication used Pre-Shared Keys as the WEP keys. The Robust Security Network (RSN) specification allows a system to use a Pre-Shared Key if there is no other authentication method available, but using a Pre-Shared Key is not as secure.

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.

RF Radio frequency. A generic term for radio-based technology.

roaming A feature of some access points that allows users to move through a facility while maintaining an unbroken connection to the LAN.

RSN Robust Security Network

RSNIE RSN Information Element

RP-TNC A connector type unique to Cisco 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, 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

slot time The amount of time a device waits after a collision before retransmitting a packet. Short slot times decrease the backoff time, which increases throughput.

spread spectrum 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.

SSID 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.

SSN Simple Security Network

SSN-PSK Authenticated Key Management using pre-shared Key over 802.1X. SSN is enabled and there exists a per-configured pre-shared key. In this mode, the station use 802.1X for key management.

T

Temporal Encryption Key Key used to encrypt data packets.

Temporal Key Combination of temporal encryption key and temporal MIC key.

Temporal MIC Key Key used to integrity check data packets

TID Traffic Identifier (802.1Q user priority value)

TKIP Temporal Key Integrity Protocol

transmit power The power level of radio transmission.

U

UNII 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.

UNII-1 Regulations for UNII devices operating in the 5.15- to 5.25-GHz frequency band.

UNII-2 Regulations for UNII devices operating in the 5.25- to 5.35-GHz frequency band.

UNII-3 Regulations for UNII devices operating in the 5.725- to 5.825-GHz frequency band.

unicast packet A single data message (packet) sent to a specific IP address.

W

WDS 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.

WEP 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.

WLSE Wireless LAN Solutions Engine. The WLSE is a specialized appliance for managing Cisco 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.

WNM Wireless Network Manager.

workstation A computing device with an installed client adapter.

WPA Wi-Fi Protected Access (WPA) is a 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.

INDEX

Beta Draft -- Cisco Confidential

Beta Draft -- Cisco Confidential