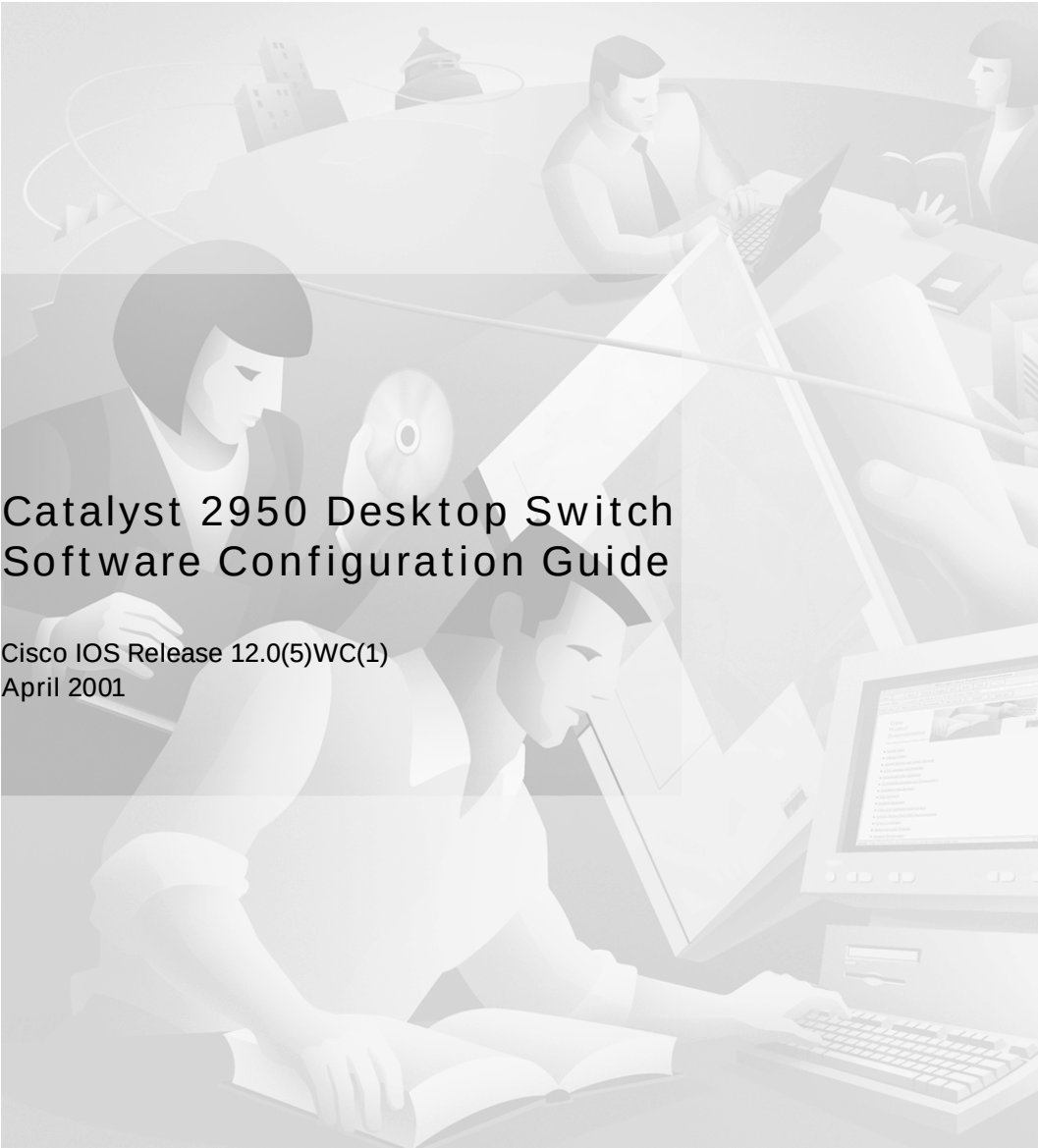




# Catalyst 2950 Desktop Switch Software Configuration Guide

Cisco IOS Release 12.0(5)WC(1)  
April 2001

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

Customer Order Number: DOC-7811380=  
Text Part Number: 78-11380-01

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

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

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

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

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

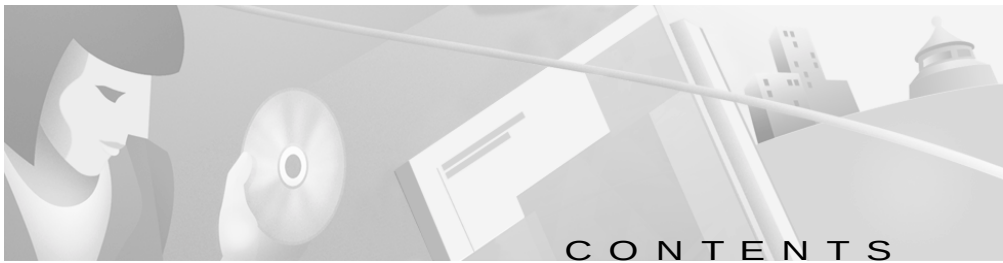
AccessPath, AtmDirector, Browse with Me, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, *CiscoLink*, the Cisco NetWorks logo, the Cisco Powered Network logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, Discover All That's Possible, Fast Step, Follow Me Browsing, FormShare, FrameShare, GigaStack, IGX, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, MGX, the Networkers logo, *Packet*, PIX, RateMUX, ScriptBuilder, ScriptShare, SlideCast, SMARTnet, TransPath, Voice LAN, Wavelength Router, WebViewer are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastSwitch, IOS, IP/TV, LightStream, MICA, Network Registrar, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries.

All other brands, names, or trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0101R)

*Catalyst 2950 Desktop Switch Software Configuration Guide*

Copyright © 2001, Cisco Systems, Inc.

All rights reserved.



# CONTENTS

## **Preface** [xv](#)

Audience and Scope [xv](#)

Organization [xv](#)

Conventions [xvi](#)

Related Publications [xvii](#)

Notes, Tips, and Cautions [xvii](#)

Obtaining Documentation [xviii](#)

World Wide Web [xviii](#)

Documentation CD-ROM [xviii](#)

Ordering Documentation [xviii](#)

Documentation Feedback [xix](#)

Obtaining Technical Assistance [xix](#)

Cisco.com [xx](#)

Technical Assistance Center [xx](#)

    Contacting TAC by Using the Cisco TAC Website [xx](#)

    Contacting TAC by Telephone [xxi](#)

---

## CHAPTER 1

## **Overview** [1-1](#)

Key Features [1-2](#)

Supported Hardware [1-3](#)

Management Options [1-4](#)

    Cisco Cluster Management Suite [1-4](#)

    IOS Command-Line Interface [1-5](#)

    SNMP Network Management Platforms [1-5](#)

- Deployment Examples [1-6](#)
  - Enterprise Workgroup Aggregation [1-6](#)
  - Small to Medium-Sized Business Workgroup Aggregation [1-7](#)

## CHAPTER 2

### Using the Management Interfaces [2-1](#)

- Preparing to Use Cluster Management Suite [2-2](#)
  - Accessing CMS for the First Time [2-2](#)
- Using the Cluster Management Suite [2-3](#)
  - Using CMS Windows [2-3](#)
  - The Common Interface of Cluster Builder and Cluster View [2-5](#)
    - Toolbar Icons for Cluster Builder and Cluster View [2-6](#)
    - Cluster View and Cluster Builder Device and Link Icons [2-7](#)
    - Menu Options for Cluster Builder and Cluster View [2-7](#)
  - Using Cluster Builder [2-9](#)
  - Using Cluster View [2-13](#)
  - Using Cluster Manager [2-14](#)
    - Menu Bar Options in Cluster Manager [2-15](#)
    - Using the Port Pop-Up Menu to Configure Ports [2-17](#)
    - Using the Device Pop-Up Menu to Configure a Switch [2-17](#)
    - Using the Cluster Tree [2-19](#)
    - Toolbar Icons for Cluster Manager [2-19](#)
  - Using VSM [2-20](#)
    - VSM Menu Bar Options [2-22](#)
    - VSM Port Pop-Up Menu and Device Pop-Up Menu Options [2-24](#)
  - Using Online Help [2-24](#)
- Using the IOS Command-Line Interface [2-24](#)
  - Understanding the CLI [2-25](#)
  - Setting Passwords and Privilege Levels [2-27](#)
  - Using the CLI to Manage Cluster Members [2-29](#)
  - Getting Help [2-30](#)

- Abbreviating Commands [2-30](#)
- Using no Commands [2-31](#)
- Understanding Command-Line Error Messages [2-31](#)
- Configuring the Switch for Telnet [2-32](#)
- Starting a Telnet Session from the Browser [2-33](#)
- Working with Files in Flash Memory [2-33](#)
- Using SNMP Management [2-34](#)
  - Using FTP to Access the MIB Files [2-35](#)
  - Using SNMP to Access MIB Variables [2-35](#)
  - Managing Cluster Switches Through SNMP [2-37](#)
  - Configuring the Switch for Remote Monitoring [2-38](#)

---

## CHAPTER 3

### **Creating and Managing Clusters [3-1](#)**

- Planning Your Cluster [3-2](#)
  - Creating Clusters with Different Releases of IOS Software [3-2](#)
  - Command Switch Requirements [3-3](#)
  - Candidate Switch Requirements [3-3](#)
  - Understanding Management VLAN Changes [3-4](#)
- Creating Clusters [3-5](#)
  - Enabling the Command Switch [3-5](#)
  - Automatically Discovering Cluster Candidates [3-6](#)
  - CLI: Creating a Cluster [3-8](#)
  - When a Cluster is Created [3-9](#)
    - Changes to the Host Name [3-10](#)
    - Changes to the SNMP Community Strings [3-10](#)
    - Changes to Passwords [3-11](#)
  - Adding and Removing Member Switches [3-12](#)
  - Determining Why a Switch Is Not Added to a Cluster [3-13](#)
  - CLI: Adding a Member to a Cluster [3-14](#)
  - CLI: Removing a Member from a Cluster [3-16](#)

|                                                               |      |
|---------------------------------------------------------------|------|
| Building a Redundant Cluster                                  | 3-17 |
| Understanding HSRP                                            | 3-18 |
| Recovering from a Failed Command Switch without HSRP          | 3-19 |
| Configuring a Cluster Standby Group                           | 3-19 |
| Standby Command Switch Requirements                           | 3-20 |
| Using the Standby Configuration Window                        | 3-20 |
| CLI: Creating a Standby Group                                 | 3-22 |
| CLI: Adding Member Switches to a Standby Group                | 3-24 |
| CLI: Removing a Switch from a Standby Group                   | 3-25 |
| CLI: Removing a Standby Group from the Network                | 3-26 |
| Managing Switch Clusters                                      | 3-27 |
| Accessing the Cluster Management Suite                        | 3-28 |
| Configuring Initial Cluster Settings                          | 3-30 |
| Arranging and Saving the Network Map                          | 3-30 |
| Changing User Settings                                        | 3-31 |
| Rearranging the Order of the Displayed Switches               | 3-31 |
| Changing the Host Name                                        | 3-32 |
| Saving Configuration Changes                                  | 3-33 |
| Displaying an Inventory of Cluster Switches                   | 3-33 |
| Displaying Link Information                                   | 3-34 |
| Changing the Management VLAN                                  | 3-34 |
| Guidelines for Changing the Management VLAN                   | 3-35 |
| Changing the Management VLAN for a Cluster                    | 3-35 |
| Changing the Management VLAN for a New Switch                 | 3-37 |
| CLI: Changing the Management VLAN Through a Telnet Connection | 3-37 |
| Monitoring and Configuring Ports                              | 3-38 |
| Monitoring Port Settings                                      | 3-39 |
| Monitoring Other Switch LEDs                                  | 3-41 |
| Guidelines for Configuring Ports                              | 3-41 |

|                                                                                |      |
|--------------------------------------------------------------------------------|------|
| Connecting to Devices That Do Not Autonegotiate                                | 3-41 |
| Configuring Ports                                                              | 3-42 |
| Port Statistics                                                                | 3-46 |
| Port Search                                                                    | 3-47 |
| CLI: Setting Speed and Duplex Parameters                                       | 3-49 |
| CLI: Configuring Flow Control on Gigabit Ethernet Ports                        | 3-49 |
| Displaying VLAN Membership                                                     | 3-50 |
| Upgrading or Reloading the Switch Software                                     | 3-51 |
| Guidelines for Upgrading or Reloading Switch Software                          | 3-51 |
| Configuring the Cisco TFTP Server to Upgrade Multiple Switches                 | 3-52 |
| CLI: Copying the Startup Configuration from the Switch to a PC or Server       | 3-52 |
| Using the Software Upgrade Page to Upgrade Switch Software                     | 3-53 |
| CLI: Upgrading a Standalone Switch                                             | 3-55 |
| CLI: Reloading or Upgrading Catalyst 2950, 2900 XL, or 3500 XL Member Switches | 3-57 |
| CLI: Upgrading Catalyst 1900 or 2820 Member Switches                           | 3-58 |
| Reloading Switch Software                                                      | 3-59 |
| Configuring SNMP for a Cluster                                                 | 3-59 |
| Enabling or Disabling the SNMP Agent                                           | 3-60 |
| Configuring Community Strings for Cluster Switches                             | 3-60 |
| Configuring Trap Managers and Enabling Traps                                   | 3-63 |

---

**CHAPTER 4****Managing Switches 4-1**

|                                              |      |
|----------------------------------------------|------|
| Finding More Information About IOS Commands  | 4-1  |
| Managing Configuration Conflicts             | 4-2  |
| Features, Default Settings, and Descriptions | 4-2  |
| Configuring Standalone Switches              | 4-9  |
| Enabling the Switch as a Command Switch      | 4-10 |
| Changing the Password                        | 4-11 |

- Creating EtherChannel Port Groups [4-11](#)
  - Understanding EtherChannel Port Grouping [4-12](#)
  - Port Group Restrictions on Static-Address Forwarding [4-14](#)
  - CLI: Creating EtherChannel Port Groups [4-15](#)
- Enabling Switch Port Analyzer [4-15](#)
  - CLI: Enabling Switch Port Analyzer [4-17](#)
  - CLI: Disabling Switch Port Analyzer [4-18](#)
- Configuring Flooding Controls [4-18](#)
  - Enabling Storm Control [4-18](#)
    - CLI: Enabling Storm Control [4-20](#)
    - CLI: Disabling Storm Control [4-21](#)
- Managing the System Date and Time [4-22](#)
  - Setting the System Date and Time [4-22](#)
  - Configuring Daylight Saving Time [4-23](#)
  - Configuring the Network Time Protocol [4-24](#)
    - Configuring the Switch as an NTP Client [4-25](#)
    - Enabling NTP Authentication [4-26](#)
    - Configuring the Switch for NTP Broadcast-Client Mode [4-26](#)
- Configuring IP Information [4-26](#)
  - Manually Assigning IP Information to the Switch [4-27](#)
    - CLI: Assigning IP Information to the Switch [4-28](#)
    - CLI: Removing an IP Address [4-29](#)
  - DHCP-Based Autoconfiguration [4-29](#)
    - DHCP Client Request Process [4-30](#)
    - Configuring the DHCP Server [4-32](#)
    - Configuring the TFTP Server [4-33](#)
    - Configuring the DNS [4-33](#)
    - Configuring the Relay Device [4-34](#)
    - Obtaining Configuration Files [4-35](#)
    - Example Configuration [4-37](#)



|                                                           |      |
|-----------------------------------------------------------|------|
| Specifying a Domain Name and Configuring the DNS          | 4-39 |
| Specifying the Domain Name                                | 4-40 |
| Specifying a Name Server                                  | 4-41 |
| Enabling the DNS                                          | 4-41 |
| Configuring SNMP                                          | 4-41 |
| Disabling and Enabling SNMP                               | 4-42 |
| Entering Community Strings                                | 4-42 |
| Adding Trap Managers                                      | 4-44 |
| CLI: Adding a Trap Manager                                | 4-47 |
| Managing the ARP Table                                    | 4-47 |
| Managing the MAC Address Tables                           | 4-49 |
| MAC Addresses and VLANs                                   | 4-50 |
| Changing the Address Aging Time                           | 4-50 |
| CLI: Configuring the Aging Time                           | 4-51 |
| CLI: Removing Dynamic Address Entries                     | 4-52 |
| Adding Secure Addresses                                   | 4-52 |
| CLI: Adding Secure Addresses                              | 4-54 |
| CLI: Removing Secure Addresses                            | 4-55 |
| Adding and Removing Static Addresses                      | 4-55 |
| Configuring Static Addresses for EtherChannel Port Groups | 4-57 |
| CLI: Adding Static Addresses                              | 4-57 |
| CLI: Removing Static Addresses                            | 4-58 |
| Enabling Port Security                                    | 4-58 |
| Defining the Maximum Secure Address Count                 | 4-60 |
| CLI: Enabling Port Security                               | 4-61 |
| CLI: Disabling Port Security                              | 4-62 |
| Configuring the Cisco Discovery Protocol                  | 4-62 |
| CLI: Configuring CDP for Extended Discovery               | 4-63 |
| IGMP Snooping                                             | 4-64 |

- Enabling or Disabling IGMP Snooping [4-66](#)
  - CLI: Enabling or Disabling IGMP Snooping [4-67](#)
  - CLI: Enabling IGMP Immediate-Leave Processing [4-68](#)
  - Setting the Snooping Method [4-69](#)
- Joining a Multicast Group [4-70](#)
  - Statically Configuring a Host to Join a Group [4-72](#)
  - CLI: Statically Configuring a Interface to Join a Group [4-75](#)
- Leaving a Multicast Group [4-76](#)
- Configuring a Multicast Router Port [4-76](#)
  - CLI: Configuring a Multicast Router Port [4-79](#)
- Configuring the Spanning Tree Protocol [4-80](#)
  - Supported STP Instances [4-80](#)
  - Using STP to Support Redundant Connectivity [4-83](#)
  - Accelerating Aging to Retain Connectivity [4-83](#)
  - Disabling STP Protocol [4-83](#)
  - CLI: Disabling STP [4-84](#)
  - Configuring Redundant Links By Using STP UplinkFast [4-84](#)
  - CLI: Enabling STP UplinkFast [4-87](#)
  - Changing STP Parameters for a VLAN [4-87](#)
    - CLI: Changing the STP Implementation [4-90](#)
    - CLI: Changing the Switch Priority [4-91](#)
    - CLI: Changing the BPDU Message Interval [4-92](#)
    - CLI: Changing the Hello BPDU Interval [4-92](#)
    - CLI: Changing the Forwarding Delay Time [4-93](#)
  - Changing STP Port Parameters [4-93](#)
    - Enabling the Port Fast Feature [4-95](#)
    - CLI: Enabling STP Port Fast [4-97](#)
    - CLI: Changing the Path Cost [4-97](#)
    - CLI: Changing the Port Priority [4-98](#)
  - CLI: Configuring STP Root Guard [4-98](#)

|                                                                            |       |
|----------------------------------------------------------------------------|-------|
| CLI: Configuring UniDirectional Link Detection                             | 4-100 |
| Configuring Protected Ports                                                | 4-100 |
| CLI: Configuring Protected Ports                                           | 4-101 |
| Configuring TACACS+                                                        | 4-101 |
| Understanding TACACS+                                                      | 4-102 |
| CLI Procedures for Configuring TACACS+                                     | 4-102 |
| CLI: Configuring the TACACS+ Server Host                                   | 4-103 |
| CLI: Configuring Login Authentication                                      | 4-104 |
| CLI: Specifying TACACS+ Authorization for EXEC Access and Network Services | 4-105 |
| CLI: Starting TACACS+ Accounting                                           | 4-106 |
| CLI: Configuring a Switch for Local AAA                                    | 4-107 |
| Configuring the Switch for Remote Monitoring                               | 4-108 |

---

## CHAPTER 5

### **Creating and Maintaining VLANs 5-1**

|                                                    |      |
|----------------------------------------------------|------|
| Number of Supported VLANs                          | 5-2  |
| VLAN Port Membership Modes                         | 5-3  |
| VLAN Membership Combinations                       | 5-3  |
| Clusters, VLAN Membership, and the Management VLAN | 5-4  |
| Assigning Static-Access Ports to a VLAN            | 5-5  |
| Using the VLAN Trunk Protocol                      | 5-6  |
| The VTP Domain                                     | 5-7  |
| VTP Modes and VTP Mode Transitions                 | 5-8  |
| VTP Advertisements                                 | 5-9  |
| VTP Version 2                                      | 5-10 |
| VTP Configuration Guidelines                       | 5-10 |
| Domain Names                                       | 5-10 |
| Passwords                                          | 5-11 |
| VTP Version                                        | 5-11 |

|                                                       |      |
|-------------------------------------------------------|------|
| Default VTP Configuration                             | 5-12 |
| Configuring VTP                                       | 5-12 |
| CLI: Configuring VTP Server Mode                      | 5-14 |
| CLI: Configuring VTP Client Mode                      | 5-15 |
| CLI: Disabling VTP (VTP Transparent Mode)             | 5-16 |
| CLI: Enabling VTP Version 2                           | 5-17 |
| CLI: Disabling VTP Version 2                          | 5-18 |
| CLI: Monitoring VTP                                   | 5-18 |
| VLANs in the VTP Database                             | 5-19 |
| Token Ring VLANs                                      | 5-20 |
| VLAN Configuration Guidelines                         | 5-20 |
| Default VLAN Configuration                            | 5-21 |
| Configuring VLANs in the VTP Database                 | 5-24 |
| CLI: Adding an VLAN                                   | 5-25 |
| CLI: Modifying a VLAN                                 | 5-26 |
| CLI: Deleting a VLAN                                  | 5-27 |
| CLI: Assigning Static-Access Ports to a VLAN          | 5-28 |
| How VLAN Trunks Work                                  | 5-29 |
| IEEE 802.1Q Configuration Considerations              | 5-30 |
| Trunks Interacting with Other Features                | 5-30 |
| Configuring a Trunk Port                              | 5-31 |
| CLI: Configuring a Trunk Port                         | 5-32 |
| CLI: Disabling a Trunk Port                           | 5-34 |
| CLI: Defining the Allowed VLANs on a Trunk            | 5-34 |
| CLI: Configuring the Native VLAN for Untagged Traffic | 5-36 |
| Configuring IEEE 802.1p Class of Service              | 5-37 |
| How Class of Service Works                            | 5-37 |
| Port Priority                                         | 5-37 |
| Port Scheduling                                       | 5-37 |
| CLI: Configuring the CoS Port Priorities              | 5-38 |

CoS and WRR [5-39](#)

CLI: Configuring CoS Priority Queues [5-42](#)

CLI: Configuring WRR [5-43](#)

Load Sharing Using STP [5-43](#)

Load Sharing Using STP Port Priorities [5-44](#)

CLI: Configuring STP Port Priorities and Load Sharing [5-45](#)

Load Sharing Using STP Path Cost [5-46](#)

CLI: Configuring STP Path Costs and Load Sharing [5-48](#)

## CHAPTER 6

### Creating Performance Graphs and Link Reports [6-1](#)

Displaying Link Graphs [6-1](#)

Displaying the Percent Utilization [6-2](#)

Displaying the Bandwidth Utilization Graph [6-2](#)

Displaying the Link Report [6-3](#)

## CHAPTER 7

### Troubleshooting [7-1](#)

Autonegotiation Mismatches [7-1](#)

Troubleshooting CMS Sessions [7-3](#)

Recovery Procedures [7-4](#)

Recovering from Corrupted Software [7-5](#)

Recovering from a Lost or Forgotten Password [7-6](#)

Recovering from a Command Switch Failure [7-8](#)

Replacing a Failed Command Switch with a Cluster Member [7-9](#)

Replacing a Failed Command Switch with Another Switch [7-12](#)

Recovering from Lost Member Connectivity [7-14](#)

## APPENDIX A

### System Error Messages [A-1](#)

How to Read System Error Messages [A-1](#)

Error Message Traceback Reports [A-4](#)

Error Message and Recovery Procedures [A-4](#)

CMP Messages [A-4](#)

Environment Messages [A-5](#)

Link Messages [A-6](#)

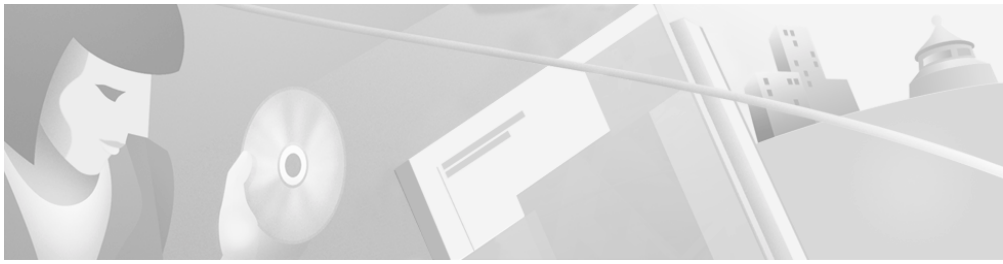
Port Security Messages [A-6](#)

RTD Messages [A-6](#)

Storm Control Messages [A-7](#)

---

INDEX



## Preface

---

The *Catalyst 2950 Desktop Switch Software Configuration Guide* describes how to configure Catalyst 2950 switches by using the command-line interface (CLI) and web-based applications. This manual refers to these switches as the Catalyst 2950 switches, or generically, as the switch.

## Audience and Scope

This guide is for the network manager responsible for configuring Catalyst 2950 switches. We assume that you are familiar with the concepts and terminology of Ethernet and local area networking.

The scope of this guide is to provide the information you need to change the configuration of a switch, create and manage clusters of switches, and troubleshoot problems that might arise.

## Organization

This guide is organized into the following chapters:

Chapter 1, “[Overview](#),” is a functional overview of the switch software. It describes Cisco IOS Release 12.0(5)WC(1) features and lists the switches that support the release. Examples show how you could deploy the switches.

Chapter 2, “[Using the Management Interfaces](#),” describes how to use the different management interfaces.

Chapter 3, “[Creating and Managing Clusters](#),” describes how to use the Cluster Management Suite (CMS) and the command-line interface (CLI) to plan and create clusters of switches. The management activities described in this chapter operate on clusters of switches.

Chapter 4, “[Managing Switches](#),” describes how to use the web-based interfaces and the CLI to configure and monitor switches. The how-to information for using the web pages in this chapter is in the online help.

Chapter 5, “[Creating and Maintaining VLANs](#),” describes how to configure VLANs in different network settings. You can configure VLANs on a single switch, by using trunk ports between switches, and by dynamically assigning VLAN membership.

Chapter 6, “[Creating Performance Graphs and Link Reports](#),” describes how to use the CMS to generate performance graphs and link reports.

Chapter 7, “[Troubleshooting](#),” describes how to identify and resolve some of the problems that might arise when you are configuring a switch running this software release.

Appendix A, “[System Error Messages](#),” describes the IOS system error messages for the Catalyst 2950 switches.

## Conventions

This publication uses the following 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 ([ ]) indicate optional elements.
- Braces ( { } ) group required choices, and vertical bars ( | ) separate the alternative elements.
- Braces and vertical bars within square brackets ([ { | } ]) indicate 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.
- Nonprinting characters, such as passwords or tabs, are in angle brackets (< >).

## Related Publications

You can order printed copies of documents with a DOC-xxxxxx= number. For more information, see the [“Obtaining Documentation” section on page xviii](#).

The following publications provide more information about the switches:

- Cisco Catalyst 2950 Desktop Switch Documentation CD

This CD is shipped with the switch and contains the following documents:

- This *Cisco IOS Desktop Switching Software Configuration Guide, Cisco IOS Release 12.0(5)WC(1)* (order number DOC-7811380=)
- *Catalyst 2950 Desktop Switch Command Reference, Cisco IOS Release 12.0(5)WC(1)* (order number DOC-7811381=)
- *Catalyst 2950 Desktop Switch Hardware Installation Guide* (order number DOC-7811157=)
- *Release Notes for the Catalyst 2950 Cisco IOS Release 12.0(5)WC(1)*

## Notes, Tips, and Cautions

Notes and cautions use the following conventions and symbols:



### Note

---

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

---



### Tips

---

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.

---

**Caution**

---

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

---

## Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

### World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- <http://www.cisco.com>
- <http://www-china.cisco.com>
- <http://www-europe.cisco.com>

### Documentation CD-ROM

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

### Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products Marketplace:

[http://www.cisco.com/cgi-bin/order/order\\_root.pl](http://www.cisco.com/cgi-bin/order/order_root.pl)

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:  
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

## Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can send us your comments by completing an online survey. When you display the document listing for this platform, click **Give Us Your Feedback**. If you are using the product-specific CD and you are connected to the Internet, click the pencil-and-paper icon in the toolbar to display the survey. After you display the survey, select the manual that you want to comment on. Click **Submit** to send your comments to the Cisco documentation group.

You can e-mail your comments to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

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

We appreciate your comments.

## Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

## Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

<http://www.cisco.com>

## Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

### Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

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

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

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

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

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

## Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

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

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.





# Overview

---

Cisco IOS Release 12.0(5)WC(1) supports the Catalyst 2950 switches. These workgroup Ethernet switches can connect 10BASE-T, 100BASE-TX, 100BASE-FX, and 1000BASE-T devices. The switches can connect to other devices as backbone switches, or they can be used in mixed configurations that connect hubs, servers, and end stations.

[Table 1-1 on page 1-3](#) lists the switches that support this switch in a cluster.

This chapter provides information on the following topics:

- Key features
- Supported hardware
- Management options
- Deployment examples

# Key Features

This section describes the key features of this software release. [Table 4-2 on page 4-3](#) lists each of these features with its default setting and a cross-reference to the section describing it. This release has the following key features:

- Automatic discovery of candidates and creation of *clusters* of up to 16 switches that can be managed through a single IP address. The Cluster Management Suite (CMS) supports:
  - Unified monitoring, configuration, and authentication of clustered switches through a web-based interface
  - Management redundancy supported by the Hot Standby Router Protocol (HSRP)
  - Extended discovery of cluster candidates for adding candidates that are not directly connected to the command switch
- Support for IEEE 802.1p class of service (CoS) scheduling for classification and preferential treatment of high-priority voice traffic
- Support for strict priority and weighted round-robin (WRR) CoS policies
- Support for the following virtual LAN (VLAN) options:
  - IEEE 802.1Q trunking support on all ports
  - Support for up to 64 VLANs
- Enhanced Spanning Tree Protocol (STP) features:
  - STP support on a per-VLAN basis
  - STP UplinkFast to accelerate the reconfiguration of STP
  - STP root guard to prevent switches outside the network core from becoming the STP root
- Terminal Access Controller Access Control System Plus (TACACS+) to manage network security through a server
- Unidirectional link detection (UDLD) support on all Ethernet ports to prevent unidirectional links
- Protected Port option for restricting the forwarding of traffic to designated ports on the same switch



- Network Time Protocol (NTP) to provide an external source for time-of-day information
- Internet Group Management Protocol (IGMP) snooping support to limit flooding of IP multicast traffic
- Dynamic Host Configuration Protocol (DHCP)-based autoconfiguration to ensure retrieval of configuration files by unicast TFTP messages

## Supported Hardware

When switches are grouped into clusters, one switch is designated as the *command switch*, and the others are *member switches*. The IP address for the entire cluster is assigned to the command switch, and it distributes configuration and management information to the others. All Catalyst 2950 switches can act as either command switches or member switches.

This section lists the switches and modules that support the Catalyst 2950 switches in a cluster environment.

**Note**

All switches can function as standalone devices.

**Table 1-1** Switches Supporting Catalyst 2950 Switches in a Cluster Configuration

| Switch Models    | Software Release          | Member Capable? | Command Capable? |
|------------------|---------------------------|-----------------|------------------|
| 2950 switches    | IOS Release 12.0(5)WC(1)  | Yes             | Yes              |
| 3500 XL switches | IOS Release 12.0(5)WC(1)  | Yes             | Yes              |
| 2900 XL switches | IOS Release               |                 |                  |
| 8 MB of DRAM     | 12.0(5)WC(1)              | Yes             | Yes              |
| 4 MB of DRAM     | 11.2(8.x)SA6 <sup>1</sup> | Yes             | No               |

**Table 1-1 Switches Supporting Catalyst 2950 Switches in a Cluster Configuration (continued)**

| Switch Models | Software Release  | Member Capable? | Command Capable? |
|---------------|-------------------|-----------------|------------------|
| 2820 switches | Release 9.00(-A)  | Yes             | No               |
|               | Release 9.00(-EN) | Yes             | No               |
| 1900 switches | Release 9.00(-A)  | Yes             | No               |
|               | Release 9.00(-EN) | Yes             | No               |

1. Original edition software. They can interoperate with this software release, but they cannot be upgraded to it.

## Management Options

This software release supports these management options:

- Cisco Cluster Management Suite
- Cisco IOS command-line interface (CLI)
- Simple Network Management Protocol (SNMP)

## Cisco Cluster Management Suite

CMS is an integrated set of web-based applications. Use these applications to create clusters of switches, monitor real-time images of the switches, and configure both clustered and standalone switches.

The three CMS applications have the following functions:

- Cluster Manager displays the front panel and LEDs of all cluster switches. Within Cluster Manager, you can point-and-click to configure ports and switches. You can select several ports from the same cluster and configure them all to run with the same settings. All of the device-management features are available through the Cluster Manager menu bar.
- Visual Switch Manager (VSM) displays the front panel of one switch. VSM is the device-management application for individual and standalone switches. When creating a cluster, you use VSM to enable the command switch.

- Cluster Builder controls discovery of cluster candidates and cluster creation. It displays a network map that uses icons to display link speeds, cluster members, cluster candidates, and edge devices. Cluster View displays a network map of the devices that are connected to a cluster, including other clusters.

A browser plug-in is required to access the CMS. For more information, refer to the *Release Notes for the Catalyst 2950 Cisco IOS Release 12.0(5)WC(1)*.

## IOS Command-Line Interface

This software release is based on Cisco IOS Release 12.0(5), but it has been enhanced to support a set of desktop-switching features. Those commands that have been added or changed for this software release are documented in this guide and in the *Catalyst 2950 Desktop Switch Command Reference*.

You can access the CLI by connecting a PC or terminal to the switch console port or by using Telnet. [Chapter 2, “Using the Management Interfaces,”](#) describes how to use the IOS CLI.

## SNMP Network Management Platforms

You can manage switches by using an SNMP-compatible management station running such platforms as HP OpenView or SunNet Manager. In a cluster configuration, the command switch manages communication between the SNMP management station and all switches in the cluster. The switch supports a comprehensive set of MIB extensions and MIB II, the IEEE 802.1D bridge MIB, and four Remote Monitoring (RMON) groups.

You can configure, monitor, and troubleshoot Catalyst 2950 switches by using the CiscoWorks2000 and CiscoView 5.0 network-management applications.

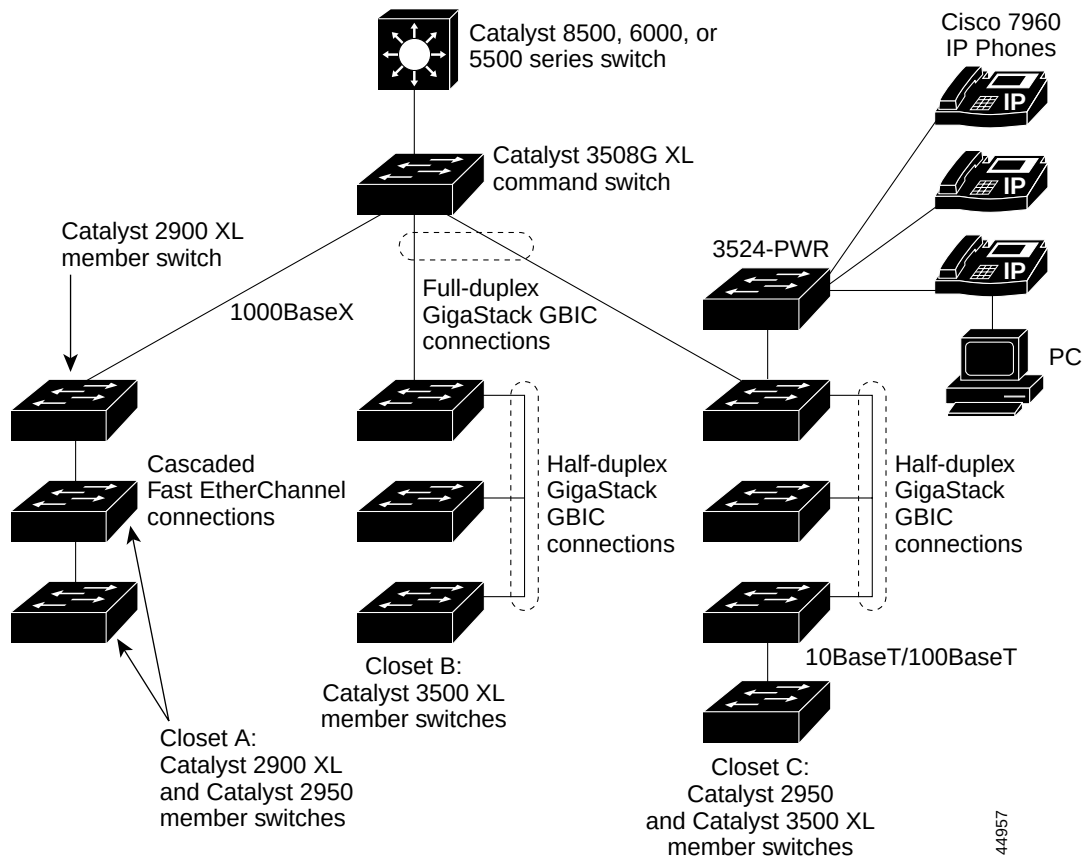
# Deployment Examples

This section describes how you can use this IOS release with the Catalyst 2950 switches.

## Enterprise Workgroup Aggregation

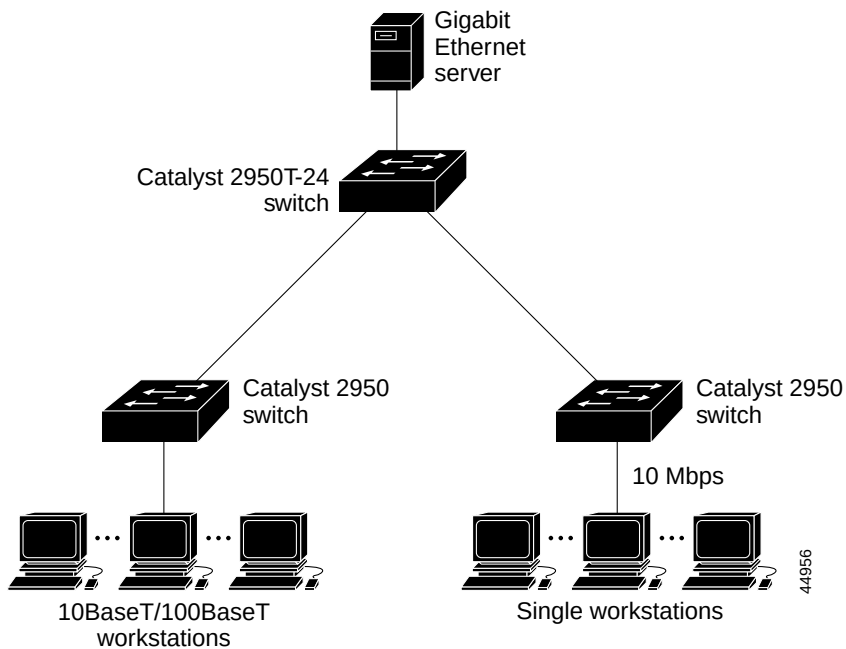
A Catalyst 3508G XL switch can be deployed to aggregate workgroup networking devices such as Ethernet 10/100 switches, 10BaseT and 10/100 hubs, workgroup servers, and Cisco 7960 IP Phones. The Catalyst 3508G XL switch can be the command switch for a single management point for the cluster. The command switch is assigned an IP address and manages other member switches (Catalyst 2950, 2900 XL, and 3500 XL) deployed in an interconnected configuration.

[Figure 1-1](#) shows such a configuration.

**Figure 1-1 Enterprise Workgroup Aggregation**

## Small to Medium-Sized Business Workgroup Aggregation

A Catalyst 2950 switch can be used in a small to medium-sized business as a network backbone. It can aggregate Ethernet and Fast Ethernet network resources in the organization and provide 1000BaseTX connections to Gigabit Ethernet servers. [Figure 1-2](#) shows such a configuration.

**Figure 1-2 Small to Medium-Sized Business Workgroup Aggregation**



## Using the Management Interfaces

---

This chapter describes the features and characteristics of the management interfaces available on the Catalyst 2950 switches. There is a command-line interface for entering IOS commands, a graphical user interface (GUI) for use with a browser such as Microsoft Internet Explorer or Netscape Navigator, and a Simple Network Management Protocol (SNMP) interface for SNMP management applications such as CiscoWorks2000 and CiscoView 5.0.

This chapter describes the following topics:

- Preparing to use the Cluster Management Suite (CMS), the HTML-based interface for configuring clusters and individual switches
- Understanding the menu options, icons, and other graphical devices that make up the CMS interface
- Understanding how to change command modes and enter commands by using the IOS command-line interface (CLI)
- Understanding how to use an SNMP management application to manage a cluster or switch



### Note

---

If you are looking for information on a specific feature, [Table 4-2 on page 4-3](#) lists the defaults for all key features and provides cross-references to feature descriptions and CLI procedures.

---

# Preparing to Use Cluster Management Suite

All of the CMS features are based on an embedded HTTP web server in the switch Flash memory.

CMS uses Hypertext Transfer Protocol (HTTP), which is an in-band form of communication with the switch through any one of its Ethernet ports and that allows switch management from a standard web browser. CMS requires that your switch uses HTTP port 80, which is the default HTTP port.

**Note**

---

If you change the HTTP port, you cannot use CMS.

---

For information about connecting to a switch port, refer to the switch hardware installation guide.

Do not disable or otherwise misconfigure the port through which your management station is communicating with the switch. You might want to write down the port number to which you are connected. Changes to the switch IP information should be done with care.

Refer to the following topics in the *Release Notes for the Catalyst 2950 Cisco IOS Release 12.0(5)WC(1)* for information about accessing CMS:

- System requirements
- Running the setup program
- Installing the required plug-in
- Configuring your web browser
- Accessing CMS

You access CMS through the default privilege level 15. For more information, see the [“Setting Passwords and Privilege Levels”](#) section on page 2-27.

## Accessing CMS for the First Time

Use the IP address of a cluster command switch or standalone switch to access the appropriate web-based application. For instructions on assigning the IP address, see the [“CLI: Assigning IP Information to the Switch”](#) section on page 4-28. For information on clustering, see [Chapter 3, “Creating and Managing Clusters.”](#)



If your network is configured with an HSRP standby group for redundancy, enter the *virtual* IP address to access CMS. See the [“Building a Redundant Cluster” section on page 3-17](#) for more information.

For detailed instructions to access Cluster Management, refer to the “Accessing CMS” section in the *Release Notes for the Catalyst 2950 Cisco IOS Release 12.0(5)WC(1)*.

## Using the Cluster Management Suite

The CMS consists of three related applications that you can use to create clusters of switches, configure and monitor switches and ports, and display link and performance information. Each cluster requires a designated command switch with an IP address to manage communication with the other switches in the cluster.

This section describes how you can use the following CMS applications to manage your network:

- Cluster Builder and Cluster View
- Cluster Manager
- Visual Switch Manager (VSM)

These CMS applications support the monitoring and configuration of all cluster and switch features. VSM supports configuration and monitoring of all device-management features for standalone switches.

All CMS applications are supported by an online help system.

## Using CMS Windows

CMS windows use consistent techniques to present and save configuration information. In some cases, CMS windows have multiple *tabs* that present different kinds of information. Tabs are arranged like folder headings across the top of the window. Click the tab to display a new screen of information, and use the Apply button to save information on all tabs without closing the window.

When you are managing a cluster of switches, a drop-down Device List at the top of the window displays the names of all cluster switches. The contents of this list can vary depending on the menu item selected. Click a switch to display the information for that switch. VSM windows, which always operate on a single switch, do not display a Device List.

Listed information can often be changed by selecting an item from a list. To change the information, select one or more items, and click **Modify**. Changing multiple items is limited to those items that apply to at least one of the selections. For example, when you select multiple ports, a parameter such as flow control is grayed out if the ports are not Gigabit Ethernet ports.



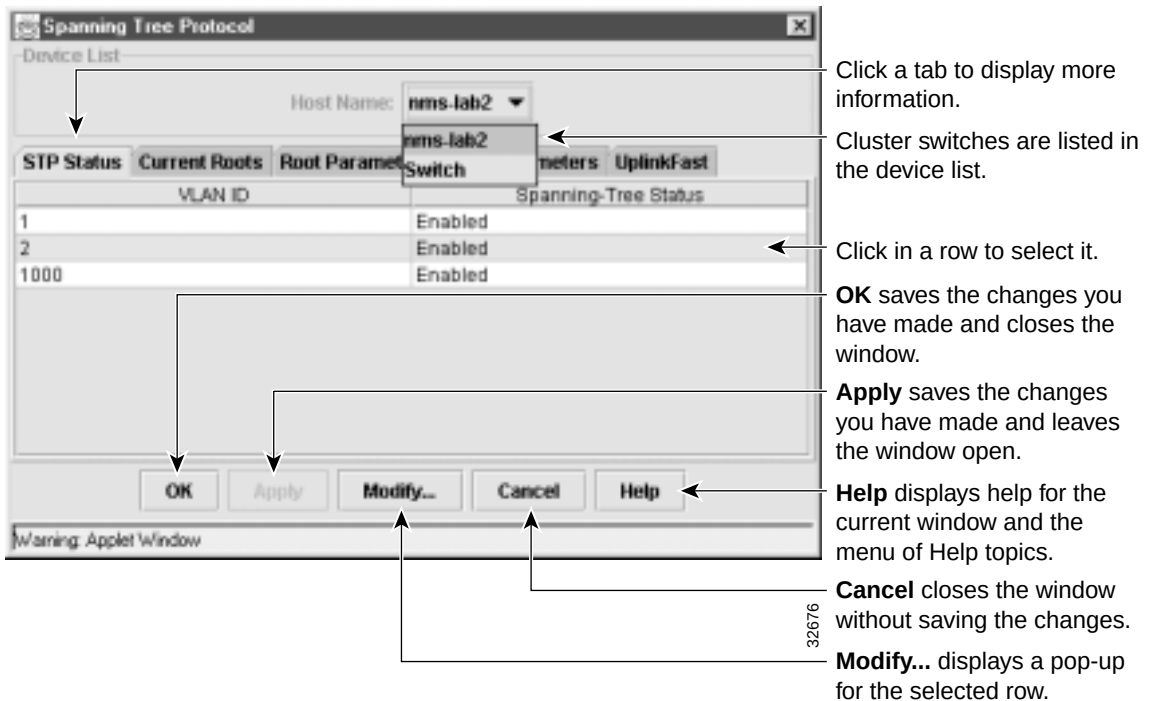
### Tips

If you try to select a port or device in Cluster Manager while there is another window still open, the computer issues a ringing bell sound. Rearrange the windows that are displayed to find the open window, and close it to proceed.

Figure 2-1 shows the components of a typical CMS window.

The following are the most common buttons that you use to control a CMS window:

| Button | Description                                                                                                                                                                                                        |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| OK     | Save any changes made in the window and close the window.                                                                                                                                                          |
| Apply  | Save any changes made in the window and leave the window open.                                                                                                                                                     |
| Cancel | Do not save any changes made in the window and close the window.                                                                                                                                                   |
| Modify | Display the pop-up for changing information on the selected item or items. You usually select an item from a list or table and click <b>Modify</b> . When you close the pop-up, you return to the original window. |
| Help   | Display the online help for the current window and the online help table of contents.                                                                                                                              |

**Figure 2-1** Components of a CMS Window

## The Common Interface of Cluster Builder and Cluster View

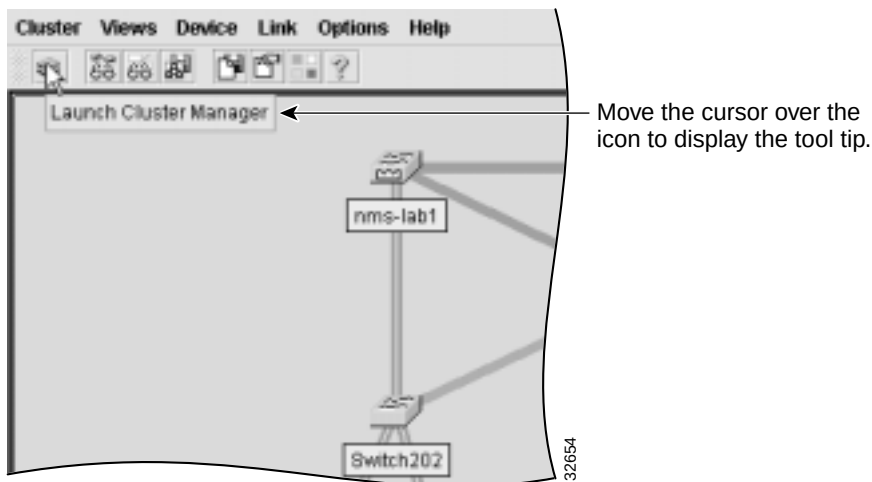
Cluster Builder and Cluster View are related applications that share the same interface. Use Cluster Builder to create and modify clusters of switches and to display a network map of their links and devices. You can create clusters with redundant command switches and display cluster members and the links between them. Cluster View displays a map of the switches in a cluster and the neighboring edge devices and clusters. Once you have displayed Cluster Builder or Cluster View, you can toggle back and forth between the two.

The user interface for Cluster Builder and Cluster View consists of the network map—the switches, links, and other devices in the cluster—and the menus and toolbar. The toolbar is a quick way to access features also available from the menu bar.

## Toolbar Icons for Cluster Builder and Cluster View

One of the ways you can configure cluster switches is by clicking a toolbar icon. [Figure 2-2](#) shows the Cluster Builder and Cluster View toolbar icons. Hold the cursor over an icon to display the feature invoked by that icon.

**Figure 2-2** Features Available Through the Toolbar



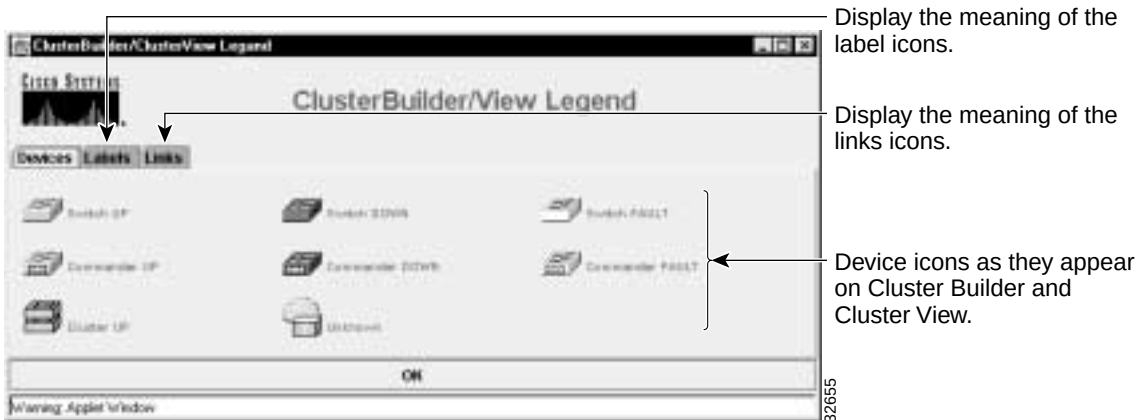
You can invoke the following features from the Cluster Builder or Cluster View toolbar (from left to right):

- Launch Cluster Manager.
- Toggle between Cluster Builder and Cluster View.
- Toggle between switch names and IP or MAC addresses and connected port numbers.
- Save the presentation of the cluster icons as you have arranged them.
- Save the current configuration for all cluster members to Flash memory.
- Set the user settings for Cluster Builder and Cluster View.
- Display the legend that describes the icons, labels, and links that are used in Cluster Builder and Cluster View.
- List the online help topics for Cluster Builder and Cluster View.

## Cluster View and Cluster Builder Device and Link Icons

The Cluster Builder and Cluster View legend shows the meaning of the colored labels and icons that represent the links and devices that make up the cluster. Select **Help > Legend** to display the legend. Figure 2-3 shows the device icons and as they display on the network map. Display the link and label icons by clicking the respective tabs.

**Figure 2-3 Icons Used in Cluster Builder and Cluster View**



## Menu Options for Cluster Builder and Cluster View

Table 2-1 lists the menu options and the tasks you can perform with Cluster Builder and Cluster View.

**Table 2-1 Menu Options for Cluster Builder and Cluster View**

| Menu Bar Choices    | Task                                                                                                                             |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------|
| <b>Cluster</b>      |                                                                                                                                  |
| Add to cluster      | Add candidates to cluster.                                                                                                       |
| Remove from cluster | Remove members from cluster.                                                                                                     |
| User Settings       | Change the default settings for the number of hops to discover and the polling interval for Cluster Builder and the link graphs. |

**Table 2-1 Menu Options for Cluster Builder and Cluster View (continued)**

| <b>Menu Bar Choices</b> | <b>Task</b>                                                                                                                                                     |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cluster Manager         | Start Cluster Manager.                                                                                                                                          |
| <b>Views</b>            |                                                                                                                                                                 |
| Toggle Views            | Toggle between Cluster Builder and Cluster View.                                                                                                                |
| Toggle Labels           | Toggle between switch names and IP or MAC addresses and connected port numbers.                                                                                 |
| <b>Device</b>           |                                                                                                                                                                 |
| Launch Switch Manager   | Start Switch Manager for a selected switch.                                                                                                                     |
| Bandwidth Graph         | Display a graph showing the current bandwidth in use by a selected switch.                                                                                      |
| Show/Hide Candidates    | Expand or collapse image of all candidates connected to a cluster member.                                                                                       |
| Host Name Configuration | Change the host name for a selected device.                                                                                                                     |
| <b>Link</b>             |                                                                                                                                                                 |
| Link Graph              | Display a graph showing the bandwidth being used for the selected link.                                                                                         |
| Link Report             | Display the Link Report for two connected devices. If one device is an unknown device, candidate, or switch, only the cluster member side of the link displays. |
| <b>Options</b>          |                                                                                                                                                                 |
| Save Layout             | Save the current presentation of the network map.                                                                                                               |
| Save Configuration      | Save the current configuration of cluster members to Flash memory.                                                                                              |
| <b>Help</b>             |                                                                                                                                                                 |
| Contents                | List all of the available online help topics.                                                                                                                   |

**Table 2-1 Menu Options for Cluster Builder and Cluster View (continued)**

| Menu Bar Choices          | Task                                                             |
|---------------------------|------------------------------------------------------------------|
| Legend                    | Display descriptions of the icons used on the network map.       |
| About ClusterBuilder View | Display the version number for Cluster Builder and Cluster View. |

## Using Cluster Builder

Follow the procedure in the “Accessing CMS” section in the *Release Notes for the Catalyst 2950 Cisco IOS Release 12.0(5)WC(1)* to display Cluster Builder. When you are using Cluster Manager, click the double-switch icon on the toolbar ([Figure 2-2](#)) to toggle back to Cluster Builder.

Use Cluster Builder to create and manage a cluster of switches. Switches connected to the command switch or cluster-capable devices display themselves as cluster members or candidates. [Figure 2-4](#) shows Cluster Builder displaying a map of cluster devices.

[Table 2-2](#) shows the meanings of the label colors in Cluster Builder. [Table 2-3](#) shows the meanings of the link colors in Cluster Builder. [Table 2-4](#) shows the meanings of the icon colors in Cluster Builder.

**Table 2-2 Device Label Color Meanings in Cluster Builder**

| Label Color | Color Meaning                                                                                                      |
|-------------|--------------------------------------------------------------------------------------------------------------------|
| Green       | A cluster member, either as a member switch or as the command switch.                                              |
| Blue        | A cluster candidate that is fully qualified to become a cluster member. Add these candidates with Cluster Builder. |
| White       | A standby command switch.                                                                                          |
| Yellow      | An unknown edge device that cannot become a member.                                                                |

**Table 2-3 Link Color Meanings in Cluster Builder**

| Link Color | Color Meaning |
|------------|---------------|
| Dark blue  | Active link   |
| Red        | Blocked link  |

**Table 2-4 Icon Color Meanings in Cluster Builder**

| Label Color | Color Meaning     |
|-------------|-------------------|
| Green       | Device is up.     |
| Red         | Device is down.   |
| Yellow      | Fault indication. |



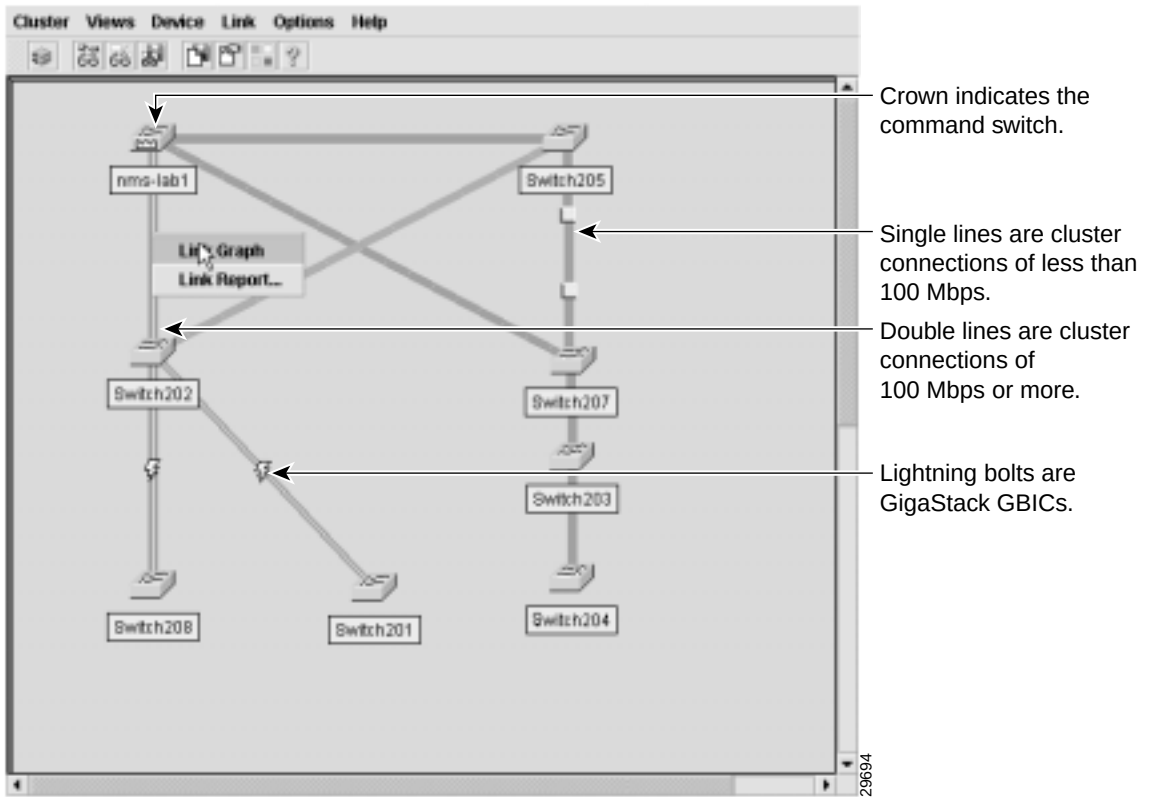
**Figure 2-4 Cluster Builder**

Table 2-5 describes the available menu options when you right-click a candidate switch.

**Table 2-5 Cluster Builder Candidate Pop-Up Menu**

| Menu Item       | Action                                                    |
|-----------------|-----------------------------------------------------------|
| Device Web Page | Displays the device-management page for the device.       |
| Add to Cluster  | Adds the selected candidate or candidates to the cluster. |

[Table 2-6](#) describes the available menu options when you right-click a member switch. For more information on configuring cluster members, see [Chapter 4, “Managing Switches.”](#)

**Table 2-6 Cluster Builder Member Pop-Up Menu**

| Menu Item           | Action                                                                                                                                                                       |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Switch Manager      | Display the VSM Home page for the selected device.                                                                                                                           |
| Bandwidth Graph     | Display a graph that plots the total bandwidth used by the switch.                                                                                                           |
| Host Name Config    | Change the name of the switch. For more information, see the <a href="#">“Changing the Host Name”</a> section on page 3-32.                                                  |
| Remove from Cluster | Remove the selected switch from the cluster.                                                                                                                                 |
| Hide Candidates     | Toggle between displaying candidate switches and not displaying them.                                                                                                        |
| Clear State         | Return switches that were down but are now up to the green (up) state. Switches that are yellow are down or were previously down. Applicable only to yellow member switches. |

[Table 2-7](#) describes the available menu options when you right-click a link. For more information on displaying link information, see [Chapter 6, “Creating Performance Graphs and Link Reports.”](#)

**Table 2-7 Cluster Builder Link Pop-Up Items**

| Menu Item   | Action                                                                                                                                                                   |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Link Graph  | Display the performance graph for the link. One end of the link must be connected to a port on a cluster member that is a Catalyst 2950, 2900 XL, or 3500 XL switch.     |
| Link Report | Displays information about the two ports in a link between members. If one end of the link is a candidate, the report only displays information about the member switch. |

## Using Cluster View

Cluster View displays a cluster as a double-switch icon with connections to edge devices and candidate switches. To access Cluster View, select **Views > Toggle Views** from the menu bar in Cluster Builder. [Table 2-8](#) describes the available menu options when you right-click an icon in Cluster View.

**Figure 2-5 Cluster View**

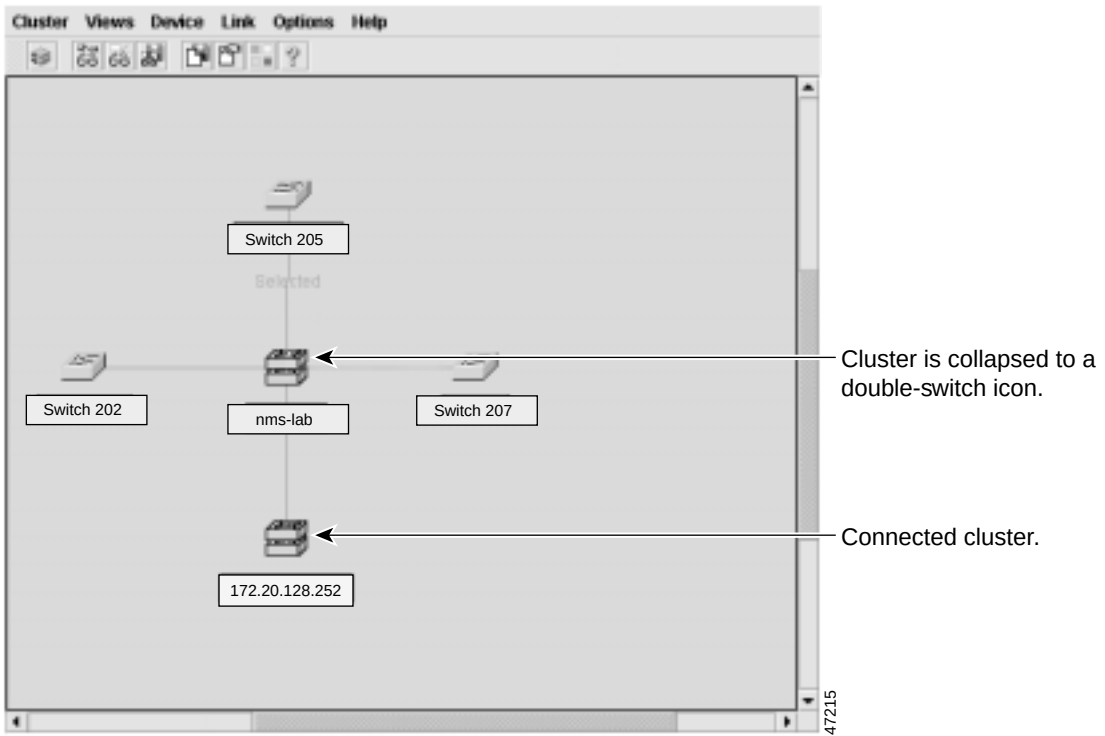


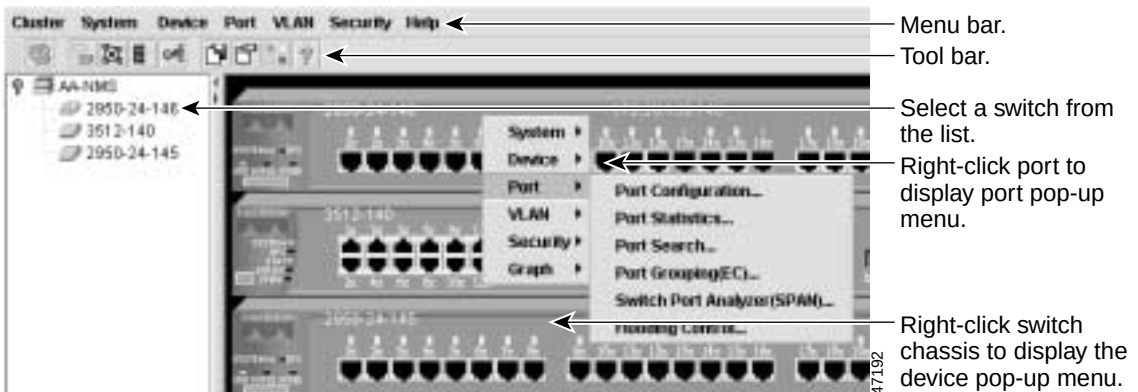
**Table 2-8 Cluster View Device Menu Options**

| Menu Item             | Action                                                         |
|-----------------------|----------------------------------------------------------------|
| Device web page       | Displays the web management page for the device.               |
| Disqualification code | Describes why the switch is not a cluster member or candidate. |

## Using Cluster Manager

For the detailed procedure to display Cluster Manager, refer to the *Release Notes for the Catalyst 2950 Cisco IOS Release 12.0(5)WC(1)*. When you are using Cluster Builder, click the double-switch icon on the toolbar (Figure 2-2) to toggle back to Cluster Manager.

Cluster Manager displays images of cluster switches that you can use to monitor and configure the devices. You can configure a cluster member on the port-, switch-, or cluster-level. With this release, many device-management features that were part of Visual Switch Manager (VSM) are available in Cluster Manager and VSM.

**Figure 2-6 Cluster Manager**

## Menu Bar Options in Cluster Manager

Table 2-9 describes the options available from the Cluster Manager menu bar.

**Table 2-9 Menu Bar Options Available in Cluster Manager**

| Menu Item                     | Task                                                                                                                                  |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| <b>Cluster</b>                |                                                                                                                                       |
| Management VLAN               | Change the management VLAN for a cluster.                                                                                             |
| System Time Management        | Configure the system time or configure the Network Time Protocol.                                                                     |
| Standby Command Configuration | Create an HSRP standby group to provide command-switch redundancy.                                                                    |
| Device Position               | Rearrange the order in which switches appear in Cluster Manager.                                                                      |
| User Settings                 | Set the polling interval for Cluster Manager, Cluster Builder, and the performance graphs. Set the application to display by default. |
| Cluster Builder               | Display Cluster Builder.                                                                                                              |
| <b>System</b>                 |                                                                                                                                       |
| Inventory                     | Display the device type, software version, IP address, and other information about a switch or a cluster of switches.                 |
| IP Management                 | Configure IP information for a switch.                                                                                                |
| Software Upgrade              | Upgrade the software for a cluster or a switch.                                                                                       |
| SNMP Management               | Enter SNMP community strings and configure end stations as trap managers.                                                             |
| Console Baud Rate             | Change the baud rate of a switch console port.                                                                                        |
| ARP Table                     | Display and maintain the Address Resolution Protocol (ARP) table.                                                                     |
| Save Configuration            | Save the configuration on one or all of the cluster switches.                                                                         |
| System Reload                 | Reboot the software on a switch or a cluster.                                                                                         |
| <b>Device</b>                 |                                                                                                                                       |
| Spanning-Tree Protocol (STP)  | Display and configure STP parameters for a switch.                                                                                    |

**Table 2-9 Menu Bar Options Available in Cluster Manager (continued)**

| Menu Item                                          | Task                                                                                                                                                |
|----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| Internet Group Management Protocol (IGMP) Snooping | Enable and disable IGMP snooping and IGMP Immediate-Leave processing on the switch. Join or leave multicast groups and configure multicast routers. |
| CoS and Weighted Round Robin (WRR)                 | Assign packets to an output queue based on their priorities. Enable WRR and assign relative weights to the output queues.                           |
| <b>Port</b>                                        |                                                                                                                                                     |
| Port Configuration                                 | Display and configure port parameters on a switch.                                                                                                  |
| Port Statistics                                    | Display detailed port statistics on link performance, dropped packets, and total errors.                                                            |
| Port Search                                        | Search for ports based on a description criteria.                                                                                                   |
| Port Grouping (EC)                                 | Group ports into logical units for high-speed links between switches.                                                                               |
| Switch Port Analyzer (SPAN)                        | Enable SPAN port monitoring.                                                                                                                        |
| Flooding Control                                   | Enable broadcast, unicast, and multicast flooding storm control.                                                                                    |
| <b>VLAN</b>                                        |                                                                                                                                                     |
| VLAN Membership                                    | Display VLAN membership, assign ports to VLANs, and configure IEEE 802.1Q trunks.                                                                   |
| VTP Management                                     | Display and configure the VLAN Trunk Protocol (VTP) for interswitch VLAN membership.                                                                |
| <b>Security</b>                                    |                                                                                                                                                     |
| Address Management                                 | Enter dynamic, secure, and static addresses into a switch address table, and define the forwarding behavior of static addresses.                    |
| Port Security                                      | Enable port security on a port.                                                                                                                     |
| <b>Help</b>                                        |                                                                                                                                                     |
| Contents                                           | List all of the available online help topics.                                                                                                       |
| Legend                                             | Display the legend that describes the icons, labels, and links.                                                                                     |
| About Cluster Manager                              | Display the version number for Cluster Manager.                                                                                                     |

## Using the Port Pop-Up Menu to Configure Ports

For port-level configuration, right-click a port to display the port pop-up menu. To configure several ports as a time, press the **Ctrl** key, and right-click ports on the same or different switches. [Table 2-10](#) describes the items available from this menu.

**Table 2-10 Cluster Manager Port Pop-up Menu**

| Menu Item          | Action When You Right-Click a Port                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Port Configuration | Configure the status, speed, duplex settings and other port-level parameters. For more information, see the <a href="#">“Monitoring and Configuring Ports”</a> section on <a href="#">page 3-38</a> .                                                                                                                                                                                               |
| VLAN Membership    | Define the VLAN mode for a port or ports, and add ports to VLANs.                                                                                                                                                                                                                                                                                                                                   |
| Flooding Controls  | Block the normal flooding of unicast and multicast packets, and enable the switch to block packet storms.                                                                                                                                                                                                                                                                                           |
| Port Security      | Enable port security on a port.                                                                                                                                                                                                                                                                                                                                                                     |
| Link Graph         | <p>Right-click a port that is green to display the performance graph for the link. You can plot the link utilization percentage and the total packets, bytes, and errors recorded on the link. For more information, see the <a href="#">“Displaying Link Graphs”</a> section on <a href="#">page 6-1</a>.</p> <p><b>Note</b> This feature is only available when selecting an individual port.</p> |

## Using the Device Pop-Up Menu to Configure a Switch

For device-level configuration, right-click the switch chassis or a switch in the cluster tree to display the device pop-up menu. The options listed on the pop-up menu are the same as those available in the drop-down menu, with the exception of the Cluster menu. [Table 2-11](#) describes the items available from this menu.

**Table 2-11 Cluster Manager Device Pop-up Menu**

| Menu Bar Choices             | Task                                                                                                                                                |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>System</b>                |                                                                                                                                                     |
| Inventory                    | Displays the device type, software version, IP address, and other information about a switch or cluster of switches.                                |
| IP Management                | Configure IP information for a switch.                                                                                                              |
| Software Upgrade             | Upgrade the software for a cluster or a switch.                                                                                                     |
| SNMP Management              | Enter SNMP community strings and configure end stations as trap managers.                                                                           |
| Console Baud Rate            | Change the baud rate for one or more switches.                                                                                                      |
| ARP Table                    | Manage the Address Resolution Protocol (ARP) table.                                                                                                 |
| Save Configuration           | Save the configuration on one or all of the cluster switches.                                                                                       |
| System Reload                | Reboot the software on a switch or a cluster.                                                                                                       |
| <b>Device</b>                |                                                                                                                                                     |
| Spanning Tree Protocol (STP) | Display and configure STP parameters for a switch.                                                                                                  |
| IGMP Snooping                | Enable and disable IGMP snooping and IGMP Immediate-Leave processing on the switch. Join or leave multicast groups and configure multicast routers. |
| CoS and WRR                  | Assign packets to an output queue based on their priorities. Enable WRR and assign relative weights to the output queues.                           |
| <b>Port</b>                  |                                                                                                                                                     |
| Port Configuration           | Display and configure port parameters on a switch.                                                                                                  |
| Port Statistics              | Display detailed port statistics on link performance, dropped packages, and total errors.                                                           |
| Port Search                  | Search for ports based on a description criteria.                                                                                                   |
| Port Grouping (EC)           | Group ports into logical units for high-speed links between switches.                                                                               |
| Switch Port Analyzer (SPAN)  | Enable SPAN port monitoring.                                                                                                                        |
| Flooding Control             | Enable broadcast, unicast, and multicast flooding storm control.                                                                                    |



**Table 2-11 Cluster Manager Device Pop-up Menu (continued)**

| Menu Bar Choices       | Task                                                                                                                                                              |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>VLAN</b>            |                                                                                                                                                                   |
| VLAN Membership        | Display VLAN membership, assign ports to VLANs, and configure IEEE 802.1Q trunks.                                                                                 |
| VTP Management         | Display and configure the VLAN Trunk Protocol (VTP) for interswitch VLAN membership.                                                                              |
| <b>Security</b>        |                                                                                                                                                                   |
| Address Management     | Enter dynamic, secure, and static addresses into a switch address table, and define the forwarding behavior of static addresses.                                  |
| Port Security          | Enable port security on a port.                                                                                                                                   |
| <b>Bandwidth Graph</b> | Display a graph that plots the total bandwidth in use by the switch. For more information, see the <a href="#">“Displaying Link Graphs” section on page 6-1</a> . |

## Using the Cluster Tree

The cluster tree displays the name of the cluster and the status of cluster members. Left-click a switch icon in the cluster tree to select it, and right-click to display the device pop-up menu.

## Toolbar Icons for Cluster Manager

You can click the toolbar icon to invoke some Cluster Manager features. As shown in [Figure 2-7](#), a description of the icon displays when you move the cursor over it.

**Figure 2-7 Cluster Manager Toolbar Icons**

Click a Cluster Manager toolbar to invoke the following features, from left to right:

- Start Cluster Builder
- Display the Software Upgrade window
- Display the SNMP Management window
- Display the VLAN Membership window
- Display the Spanning Tree Protocol window
- Display the Save Configuration window
- Display the User Settings window
- Display the legend that describes the icons, labels, and links
- Display the Help table of contents. (See [Using Online Help, page 2-24](#))

## Using VSM

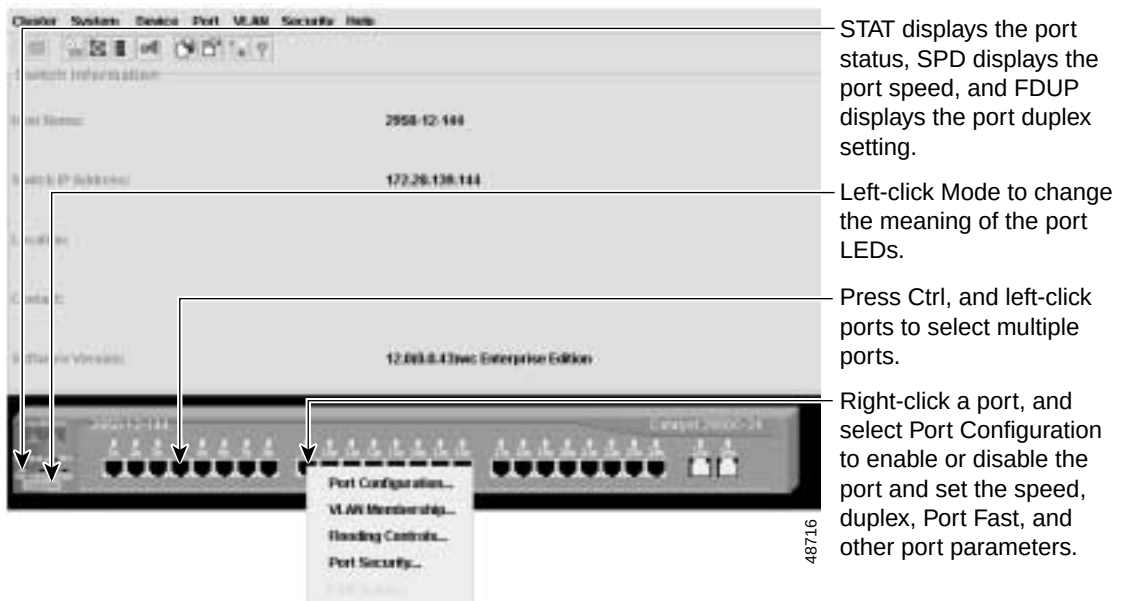
VSM is a web-based device-management application for configuring and monitoring a clustered or standalone switch. If your switch is part of a cluster, you can also perform many VSM tasks from within Cluster Manager.

For the detailed procedure to display VSM, refer to the *Release Notes for the Catalyst 2950 Cisco IOS Release 12.0(5)WC(1)*. To display VSM from within Cluster Builder or Cluster View, click a switch, and select **Device > Launch Switch Manager** from the menu bar.

The VSM Home page displays a real-time image of the switch that you can use to monitor and reconfigure the switch and switch ports. The images of the LEDs displayed by VSM convey the same information as the LEDs on the front panel of the switch. You can configure a port or ports by right-clicking them and selecting a item from the Port Pop-Up menu.

When you use VSM to reconfigure a switch, the change becomes part of the *running configuration* of the switch. The image of the switch and VSM windows always display the switch running configuration. However, the running configuration is not necessarily the startup configuration that is used when the switch restarts. To ensure that your changes are saved after a restart in VSM, select **System > Save Configuration** from the menu bar. If you are using the CLI, you can save the configuration by entering the **write memory** command in privileged EXEC mode.

**Figure 2-8 VSM Home Page**



## VSM Menu Bar Options

You can access the device-management features from the Home page menu bar. [Table 2-12](#) describes the menu options and their function.

**Table 2-12 Menu Bar Options Available in VSM**

| Menu Bar Choices              | Task                                                                                                                                                |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Cluster</b>                |                                                                                                                                                     |
| Cluster Command Configuration | Enable a switch to act as the cluster command switch.                                                                                               |
| Cluster Management            | Display Cluster Manager or Cluster Builder.                                                                                                         |
| <b>System</b>                 |                                                                                                                                                     |
| Inventory                     | Display the device type, software version, IP address, and other information about a switch.                                                        |
| IP Management                 | Configure IP information for a switch.                                                                                                              |
| Software Upgrade              | Upgrade the software for the cluster or a switch.                                                                                                   |
| System Time Management        | Configure the system time or the Network Time Protocol (NTP).                                                                                       |
| SNMP Management               | Enter SNMP community strings and configure end stations as trap managers.                                                                           |
| Console Baud Rate             | Change the baud rate for a switch.                                                                                                                  |
| ARP Table                     | Display the device Address Resolution Protocol (ARP) table.                                                                                         |
| User Settings                 | Change the polling intervals for clustering and graphing, and enable the display of the splash page when VSM starts.                                |
| Save Configuration            | Save the configuration.                                                                                                                             |
| System Reload                 | Reboot the software on a switch.                                                                                                                    |
| <b>Device</b>                 |                                                                                                                                                     |
| Spanning-Tree Protocol (STP)  | Display and configure STP parameters for a switch.                                                                                                  |
| IGMP Snooping                 | Enable and disable IGMP snooping and IGMP Immediate-Leave processing on the switch. Join or leave multicast groups and configure multicast routers. |

**Table 2-12 Menu Bar Options Available in VSM (continued)**

| Menu Bar Choices            | Task                                                                                                                                      |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| CoS and WRR                 | Assign packets to an output queue based on their priorities. Enable WRR and assign relative weights to the output queues.                 |
| <b>Port</b>                 |                                                                                                                                           |
| Port Configuration          | Display and configure port parameters on a switch.                                                                                        |
| Port Statistics             | Display detailed port statistics on link performance, dropped packages, and total errors.                                                 |
| Port Search                 | Search for ports based on a description criteria.                                                                                         |
| Port Grouping (EC)          | Group ports into logical units for high-speed links between switches.                                                                     |
| Switch Port Analyzer (SPAN) | Enable SPAN port monitoring.                                                                                                              |
| Flooding Control            | <b>Note</b> Enable broadcast, unicast, and multicast flooding storm control.                                                              |
| <b>VLAN</b>                 |                                                                                                                                           |
| VLAN Membership             | Display VLAN membership, assign ports to VLANs, and configure 802.1Q trunks.                                                              |
| Management VLAN             | Change the management VLAN on the switch.                                                                                                 |
| VTP Management              | Display and configure the VLAN Trunk Protocol (VTP) for interswitch VLAN membership.                                                      |
| <b>Security</b>             |                                                                                                                                           |
| Address Management          | Enter dynamic, secure, and static addresses into a switch address table. You can also define the forwarding behavior of static addresses. |
| Port Security               | Enable port security on a port.                                                                                                           |
| <b>Help</b>                 |                                                                                                                                           |
| Contents                    | List all of the available online help topics.                                                                                             |
| Legend                      | Display the legend that describes the icons, labels, and links.                                                                           |
| About Visual Switch Manager | Display the version number for Visual Switch Manager.                                                                                     |

## VSM Port Pop-Up Menu and Device Pop-Up Menu Options

The options available through the port pop-up and device pop-up menus in VSM are the same as those described in [Table 2-10](#) and [Table 2-11](#).

## Using Online Help

To get online help for CMS, do either of the following:

- Select **Help > Contents** from the menu bar. The left pane of the Help window displays the **Contents** tab of the help system. The right pane displays information for the first topic on the tab.
- Click **Help** in whatever CMS window you are using. The left pane of the Help window displays the **Contents** tab, positioned to the topic for the CMS window. The right pane displays information on how to use the CMS window.

You can navigate within the Help window to find whatever CMS information you need. By expanding the topics on the **Contents** tab and scrolling, you can see the breadth of topics in the help system. Double-click any one, and information for it appears in the right pane. A glossary is also available; it is the bottom topic on the tab. You can also find information by clicking the **Index** tab. Use its entry field and **Find** button to look for a specific entry, or scroll until you find what you need. Double-click an index entry, and information for it appears in the right pane.

In addition to these navigation features, the online help offers:

- **Backward** and **Forward** buttons to let you review previous topics and return.
- Numerous links within the help topics—links from concepts to task details and from highlighted terms to glossary entries.

## Using the IOS Command-Line Interface

This section introduces the Cisco IOS command-line interface (CLI). The *Catalyst 2950 Desktop Switch Command Reference* contains a complete description of commands that have been created or changed for the Catalyst 2950 switches.

This section describes how to perform the following tasks:

- Understand the CLI and its command modes
- Use the CLI to manage member switches
- Set passwords
- Configure the switch for Telnet
- Work with files in Flash memory

**Note**

---

Certain port features can conflict with one another. Review the [“Managing Configuration Conflicts” section on page 4-2](#) before you change the port settings.

---

## Understanding the CLI

This section describes the Cisco IOS command-mode structure. Each command mode supports specific Cisco IOS commands. For example, the **interface** command is used only from global configuration mode.

The switch supports the following command modes:

- User EXEC
- Privileged EXEC
- VLAN database
- Global configuration
- Interface configuration
- Line configuration

[Table 2-13](#) describes how to access each mode, the prompt you see in that mode, and how to exit the mode. The examples in the table use the host name *switch*.

**Table 2-13 Command Modes Summary**

| Modes                | Access Method                                                         | Prompt          | Exit Method                                                                                 | About This Mode <sup>1</sup>                                                                                                                                          |
|----------------------|-----------------------------------------------------------------------|-----------------|---------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| User EXEC            | Begin a session with your switch.                                     | switch>         | Enter <b>logout</b> or <b>quit</b> .                                                        | Use this mode to <ul style="list-style-type: none"> <li>• Change terminal settings.</li> <li>• Perform basic tests.</li> <li>• Display system information.</li> </ul> |
| Privileged EXEC      | Enter the <b>enable</b> command while in user EXEC mode.              | switch#         | Enter <b>disable</b> to exit.                                                               | Use this mode to verify commands you have entered. Access to this mode should be protected with a password.                                                           |
| VLAN database        | Enter the <b>vlan database</b> command while in privileged EXEC mode. | switch(vlan)#   | To exit to privileged EXEC mode, enter <b>exit</b> .                                        | Use this mode to configure VLAN-specific parameters.                                                                                                                  |
| Global configuration | Enter the <b>configure</b> command while in privileged EXEC mode.     | switch(config)# | To exit to privileged EXEC mode, enter <b>exit</b> or <b>end</b> , or press <b>Ctrl-Z</b> . | Use this mode to configure parameters that apply to your switch as a whole.                                                                                           |



**Table 2-13 Command Modes Summary (continued)**

| Modes                   | Access Method                                                                                              | Prompt               | Exit Method                                                                                                                           | About This Mode <sup>1</sup>                                       |
|-------------------------|------------------------------------------------------------------------------------------------------------|----------------------|---------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|
| Interface configuration | Enter the <b>interface</b> command (with a specific interface) while in global configuration mode.         | switch(config-if)#   | To exit to global configuration mode, enter <b>exit</b> .<br><br>To exit to privileged EXEC mode, enter <b>Ctrl-Z</b> or <b>end</b> . | Use this mode to configure parameters for the Ethernet interfaces. |
| Line configuration      | Specify a line with the <b>line vty</b> or <b>line console</b> command while in global configuration mode. | switch(config-line)# | To exit to global configuration mode, enter <b>exit</b> .<br><br>To exit to privileged EXEC mode, enter <b>Ctrl-Z</b> or <b>end</b> . | Use this mode to configure parameters for the terminal line.       |

1. For any of the modes, you can see a comprehensive list of the available commands by entering a question mark (?) at the prompt.

## Setting Passwords and Privilege Levels

Because many privileged EXEC commands are used to set operating parameters, you should password-protect these commands to prevent unauthorized use.

Catalyst 2950 switches have two commands for setting passwords:

- **enable secret** *password* (a very secure, encrypted password)
- **enable password** *password* (a less secure, unencrypted password)

You must enter one of these passwords to gain access to privileged EXEC mode. It is recommended that you use the enable secret password.

If you enter the **enable secret** command, the text is encrypted before it is written to the config.text file, and it is unreadable. If you enter the **enable password** command, the text is written as entered to the config.text file where you can read it.

**Note**

---

When set, the enable secret password takes precedence, and the enable password serves no purpose.

---

Both types of passwords can contain from 1 to 25 uppercase and lowercase alphanumeric characters, and both can start with a number. Spaces are also valid password characters; for example, *two words* is a valid password. Leading spaces are ignored; trailing spaces are recognized. The password is case sensitive.

To remove a password, use the **no** version of the commands: **no enable secret** or **no enable password**. If you lose or forget your enable password, see the [“Recovering from a Lost or Forgotten Password” section on page 7-6](#).

When the Cluster Builder suggests a candidate to add to a cluster, you enter the password of the candidate switch, if one was defined, and the switch joins the cluster. Then the member switch inherits the command switch password. For more information on managing passwords for the Cluster Management Suite, see the [“Changes to Passwords” section on page 3-11](#).

You can also specify up to 15 privilege levels and define passwords for them by using the **enable password [level level] {password}** or **enable secret [level level] {password}** command. Level 1 is normal EXEC-mode user privileges. If you do not specify a level, the privilege level defaults to 15 (traditional enable privileges).

**Note**

---

You need privilege level 15 to access VSM and the Cluster Management Suite. You must also use privilege level 15 if you configure the TACACS+ (Terminal Access Controller Access Control System Plus) protocol from the CLI so that all your HTTP connections will be authenticated through the TACACS+ server.

---

You can specify a level, set a password, and 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 information on other IOS Release 12.0 commands, refer to the Cisco IOS Release 12.0 documentation set available on Cisco.com.

## Using the CLI to Manage Cluster Members

You can configure member switches from the CLI by first logging into the command switch. Enter the EXEC mode **rcommand** command and the member switch number to start a Telnet session (through a console or Telnet connection) and access the member switch CLI. Except when connecting to a Catalyst 1900 or 2820 switch running standard edition software with the command switch at privilege level 1 to 14, you are not prompted for a password because the member switch inherited the password of the command switch when it joined the cluster.

The following example shows how to log into member-switch 3 from the command-switch CLI:

```
switch# rcommand 3
```

If you do not know the member-switch number, enter the EXEC mode **show cluster members** command on the command switch.

For Catalyst 2950 switches, the Telnet session accesses the member-switch CLI at the same privilege level as on the command switch. The IOS commands then operate as usual. For instructions on configuring the Catalyst 2950 switch for a Telnet session, see the [“Configuring the Switch for Telnet” section on page 2-32](#).

For Catalyst 1900 and 2820 switches running standard edition software, the Telnet session accesses the menu console (the menu-driven interface) if the command switch is at privilege level 15. If the command switch is at privilege level 14, you are prompted for the password before being able to access the menu console.

Command switch privilege levels map to the Catalyst 1900 and 2820 member switches running standard and Enterprise Edition Software as follows:

- If the command switch privilege level is 1 to 14, the member switch is accessed at privilege level 1.
- If the command switch privilege level is 15, the member switch is accessed at privilege level 15.

The Catalyst 1900 and 2820 CLI is available only on switches running Enterprise Edition Software.

## Getting Help

You can use the question mark (?) and arrow keys to help you enter commands.

For a list of available commands in a command mode, enter a question mark:

```
switch> ?
```

To complete a command, enter a few known characters followed by a tab (with no space):

```
switch# sh conf<tab>  
switch# sh configuration
```

For a list of command variables, enter the command followed by a space and a question mark:

```
switch> show ?
```

To redisplay a command you previously entered, press the up-arrow key. You can continue to press the up-arrow key for more commands.

## Abbreviating Commands

You only have to enter enough characters for the switch to recognize the command as unique. This example shows how to enter the **show configuration** command:

```
switch# show conf
```

## Using no Commands

The word *no* creates a **no** form of a command. The **no** form of a command does the following:

- Resets a command to its default values.
- or
- Reverses the action of a command. For example, the command **no shutdown** reverses the shutdown of an interface.

## Understanding Command-Line Error Messages

Table 2-14 lists some error messages that you might encounter while using the CLI to configure your switch.

**Table 2-14 Common CLI Error Messages**

| Error Message                           | Meaning                                                                          | How to Get Help                                                                                                                                                                   |
|-----------------------------------------|----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| % Ambiguous command: "show con"         | You did not enter enough characters for your switch to recognize the command.    | Reenter the command followed by a space and a question mark (?).<br><br>The possible keywords that you can enter with the command are displayed.                                  |
| % Incomplete command.                   | You did not enter all of the keywords or values required by this command.        | Reenter the command followed by a space and a question mark (?).<br><br>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 of the commands that are available in this command mode.<br><br>The possible keywords that you can enter with the command are displayed. |

## Configuring the Switch for Telnet

Follow these steps to configure a Telnet password:

|        | Command                                   | Purpose                                                                                                                                                                                                            |
|--------|-------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 |                                           | Attach a PC or workstation with emulation software to the switch console port.<br><br>The default data characteristics of the console port are 9600, 8, 1, no parity. When the command line appears, go to Step 2. |
| Step 2 | <b>enable</b>                             | Enter privileged EXEC mode.                                                                                                                                                                                        |
| Step 3 | <b>config terminal</b>                    | Enter global configuration mode.                                                                                                                                                                                   |
| Step 4 | <b>line vty 0 15</b>                      | Enter the interface configuration mode for the Telnet interface.<br><br>There are 16 possible sessions on a command-capable switch. The 0 and 15 mean that you are configuring all 16 possible Telnet sessions.    |
| Step 5 | <b>password</b> <i>&lt;password&gt;</i>   | Enter a password.                                                                                                                                                                                                  |
| Step 6 | <b>end</b>                                | Return to privileged EXEC mode so that you can verify the entry.                                                                                                                                                   |
| Step 7 | <b>show running-config</b>                | Display the running configuration.<br><br>The password is listed under the command <b>line vty 0 15</b>                                                                                                            |
| Step 8 | <b>copy running-config startup-config</b> | (Optional) Save the running configuration to the startup configuration.                                                                                                                                            |

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## Starting a Telnet Session from the Browser

Follow this procedure to start a Telnet session by using a browser:

- 
- Step 1** Start one of the supported browsers.
  - Step 2** In the **URL** field, enter the IP address of the command switch.
  - Step 3** When the Cisco Systems Access page appears, click **Telnet - to the switch** to start the Telnet session.
- 

## Working with Files in Flash Memory

You can use the file system in Flash memory to copy files and to troubleshoot configuration problems. This could be useful if you wanted to save configuration files on an external server in case a switch fails. You can then copy the configuration file back to a replacement switch and avoid having to reconfigure the switch.

As in the following example, use the privileged EXEC **dir flash:** command to display the contents of Flash memory:

```
Switch#dir
Directory of flash:/
 3  drwx      10176  Mar 01 2001 00:04:34  html
 6  -rwx       2343  Mar 01 2001 03:18:16  config.text
171 -rwx     1667997  Mar 01 2001 00:02:39  c2950-c3h2s-mz.120-5.WC.1.bin
 7  -rwx       3060  Mar 01 2001 00:14:20  vlan.dat
172 -rwx        100  Mar 01 2001 00:02:54  env_vars

7741440 bytes total (4788224 bytes free)
```

The file system uses a URL-based file specification. The following example uses the TFTP protocol to copy the file config.text from the host *arno* to the switch Flash memory:

```
switch# copy tftp://arno//2950/config.text flash:config.text
```

You can enter the following parameters as part of a filename:

- TFTP
- Flash
- RCP
- XMODEM

Use the **copy running-config startup-config** command to save your configuration changes to Flash memory so that they are not lost if there is a system reload or power outage. This example shows how to use this command to save your changes:

```
switch# copy running-config startup-config  
Building configuration...
```

It might take a minute or two to save the configuration to Flash memory. After it has been saved, the following message appears:

```
[OK]  
switch#
```

## Using SNMP Management

This section describes how to access Management Information Base (MIB) objects to configure and manage your switch. It provides the following information:

- Using FTP to access the MIB files
- Using Simple Network Management Protocol (SNMP) to access the MIB variables
- Managing cluster switches through SNMP



### Note

---

When configuring your switch by using SNMP, note that certain combinations of port features create configuration conflicts. For more information, see the [“Managing Configuration Conflicts” section on page 4-2](#).

---

CiscoWorks2000 and CiscoView 5.0 are network-management applications you can use to configure, monitor, and troubleshoot Catalyst 2950 switches.



## Using FTP to Access the MIB Files

You can obtain each MIB file with the following procedure:

- 
- 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/supportlists`.
- Step 5** Change directories to one of the following:
- `wsc2900xl` for a list of 2900 XL MIBs
  - `wsc3500xl` for a list of 3500 XL MIBs
  - `wsc2950` for a list of 2950 MIBs
- Step 6** Use the `get MIB_filename` command to obtain a copy of the MIB file.
- 

You can also access this server from your browser by entering the following URL in the **Location** field of your Netscape browser (the **Address** field in Internet Explorer):

**ftp://ftp.cisco.com**

Use the mouse to navigate to the folders listed above.

## Using SNMP to Access MIB Variables

The switch MIB variables are accessible through SNMP, an application-layer protocol facilitating the exchange of management information between network devices. The SNMP system consists of three parts:

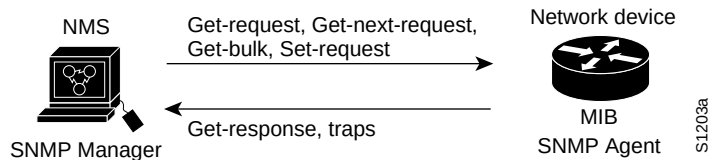
- The SNMP manager, which resides on the network management system (NMS)
- The SNMP agent, which resides on the switch
- The MIBs that reside on the switch but that can be compiled with your network management software

An example of an NMS is the CiscoWorks network management software. CiscoWorks2000 software uses the switch 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 in order to troubleshoot internetworking problems, increase network performance, verify the configuration of devices, monitor traffic loads, and more.

As shown in [Figure 2-9](#), the SNMP agent gathers data from the MIB, which is the repository for information about device parameters and network data. The agent can send traps, or 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), and so forth. In addition, the SNMP agent responds to MIB-related queries sent by the SNMP manager in *get-request*, *get-next-request*, and *set-request* format.

The SNMP manager uses information in the MIB to perform the operations described in [Table 2-15](#).

**Figure 2-9 SNMP Network**



S1203a

**Table 2-15 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. <sup>1</sup>                                           |
| 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 indicating that 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.

## Managing Cluster Switches Through SNMP

SNMP must be enabled for the Cluster Management reporting and graphing features to function properly. When you power-on your Catalyst 2950 switch for the first time, SNMP is enabled if you enter the IP information by using the setup program and accept its proposed configuration. If you did not use the setup program to enter the IP information and SNMP was not enabled, you can enable it on the SNMP Configuration page described in the [“Configuring SNMP” section on page 4-41](#). On Catalyst 1900 and 2820 switches, SNMP is enabled by default.

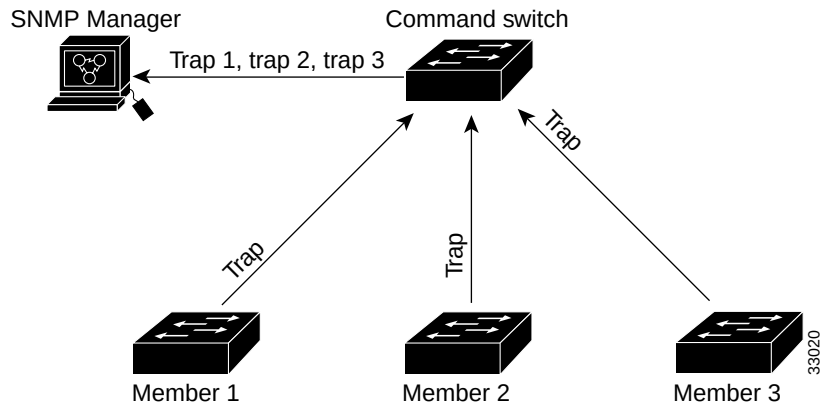
When a cluster is created, the command switch manages the exchange of messages between member switches and an SNMP application. The Cluster Management software appends the member switch number (@esN, where N is the switch number) to the first configured RW and RO community strings on the command switch and propagates them to the member switch. The command switch uses this community string to control the forwarding of gets, sets, and get-next messages between the SNMP management station and the member switches.

**Note**

When a standby group is configured, the command switch can change without your knowledge. Use the first read-write and read-only community strings to communicate with the command switch if there is a standby group configured for the cluster.

If the member switch does not have an IP address, the command switch passes traps from the member switch to the management station, as shown in [Figure 2-10](#). If a member switch has its own IP address and community strings, they can be used in addition to the access provided by the command switch. For more information, see the [“Changes to the SNMP Community Strings”](#) section on [page 3-10](#) and the [“Configuring SNMP”](#) section on [page 4-41](#).

**Figure 2-10 SNMP Management for a Cluster**



## Configuring the Switch for Remote Monitoring

This IOS software release supports four Remote Monitoring (RMON 1) groups. You can configure these groups by using an SNMP application or by using the CLI. The four supported groups are alarms, events, history, and statistics.



## Creating and Managing Clusters

---

A cluster is a group of connected switches that are managed as a single entity. The switches can be in the same location, or they can be distributed across a contiguous Layer 2 network. All communication with cluster switches is through one IP address.



### Tips

---

You can have up to 16 switches in a cluster: 1 *command* switch and up to 15 *member* switches. The command switch is the single point of access used to manage, configure, and monitor the member switches.

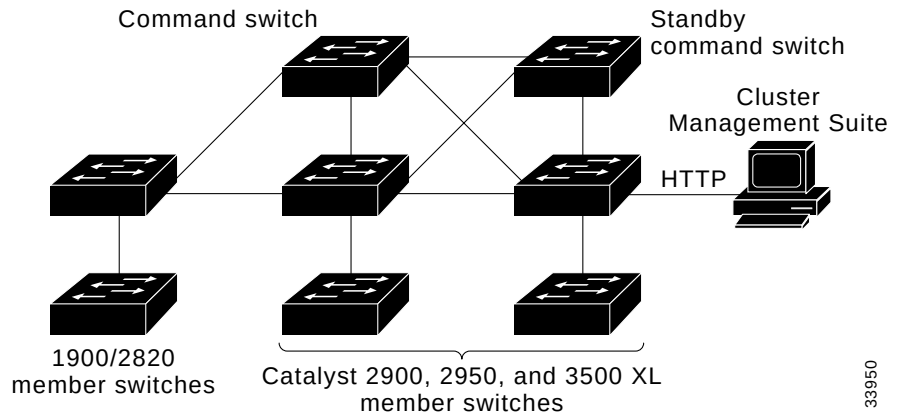
---

Clusters can be configured for management redundancy by using the Hot Standby Router Protocol (HSRP). [Figure 3-1](#) shows a cluster of switches with a standby command switch.

This chapter describes how to create and manage clusters of switches by using the Cluster Management Suite (CMS) applications: Cluster Builder, Cluster View, and Cluster Manager. You use Cluster Builder to create the cluster, you use Cluster View to display the devices connected to the cluster, and you use Cluster Manager to configure and monitor your cluster after it has been created.

This chapter describes how to perform the following tasks:

- Planning your cluster
- Creating a cluster
- Building a redundant cluster
- Managing a cluster

**Figure 3-1 A Cluster with a Standby Command Switch**

33950

## Planning Your Cluster

Anticipating conflicts and compatibility issues is a high priority when you manage several switches through a cluster. This section describes the requirements and caveats that you should understand before you create the cluster.

Before you create a cluster, you might want to consider creating a cluster with a redundant command switch. Cluster redundancy is described in the [“Building a Redundant Cluster”](#) section on page 3-17.

## Creating Clusters with Different Releases of IOS Software

Some versions of the Catalyst 2900 and 3500 XL software do not support clustering, and other versions do not support the features in this release. To ensure that all cluster switches are operating with the same level of software, we recommend that you upgrade all cluster switches to IOS Release 12.0(5)WC(1).



### Note

Catalyst 1900 and 2820 switches are always member switches.

## Command Switch Requirements

You must select a switch to be the command switch of your cluster. The command switch must satisfy the following requirements:

- It is running Cisco IOS Release 12.0(5)XU or later. See [“Supported Hardware” section on page 1-3](#) for a list of switches that can run these versions.

**Note**

If you are running Cisco IOS Release 12.0(5)XW or earlier, a Catalyst 2950 switch will show as an unknown device in Cluster Manager. In this case, you will need to use Visual Switch Manager (VSM) to manage the Catalyst 2950 switch.

- It is assigned an IP address.
- It has Cisco Discovery Protocol (CDP) version 2 enabled (the default).
- It is not a command or member switch of another cluster.
- It belongs to the same management virtual LAN (VLAN) as the cluster member switches.
- No access lists have been defined for the switch. Access lists can restrict access to a switch but are not usually used in configuring Catalyst 2950, 2900 XL, or 3500 XL switches. (This does not include access class 199 that is created when a device is configured as the command switch.)

**Note**

To avoid losing contact with cluster members when a command switch fails, you might want to create a redundant cluster. For more information, see the [“Building a Redundant Cluster” section on page 3-17](#).

## Candidate Switch Requirements

Before adding a candidate switch to the cluster, you must know any assigned enable or enable secret password.

A candidate switch must satisfy the following requirements to join a cluster.

- It is running cluster-capable software. See the [“Supported Hardware” section on page 1-3](#) for a list of switches that support clustering.
- It has CDP version 2 enabled.
- It is connected to a command switch through ports that belong to the same management VLAN (see [“Changing the Management VLAN” section on page 3-34](#)).
- It is not an active member or command switch of another cluster.

A candidate switch can have an IP address, but it is not required.

**Note**

---

If you are unable to maintain management contact with a member, see the [“Recovering from Lost Member Connectivity” section on page 7-14](#).

---

## Understanding Management VLAN Changes

Communication with the switch management interfaces is through the switch IP address. The IP address is associated with the management VLAN, which by default is VLAN 1. To manage switches in a cluster, the port connections among the command, member, and candidate switches must be connected through ports that belong to the management VLAN.

You can change the management VLAN on an existing cluster, and the command switch synchronizes activities with member switches to ensure that no loss of management connectivity occurs.

**Note**

---

This is only valid for IOS Release 12.0(5)XU and later. Previous releases of the software require that switches be upgraded one at a time.

---

To change the management VLAN on an existing cluster, see the [“Changing the Management VLAN” section on page 3-34](#).

If you add a new switch to an existing cluster and the cluster is using a management VLAN other than the default VLAN 1, the command switch automatically senses that the new switch has a different management VLAN and has not been configured. The command switch issues commands to change the management VLAN and change the port on the new switch, which is connected



to the cluster, to match the one in use by the cluster. This automatic change of the VLAN only occurs for new, out-of-box switches that do not have a config.text file and for which there have been no changes to the running configuration.

## Creating Clusters

You create a cluster by performing these tasks:

1. Cabling together switches running clustering software
2. Assigning an IP address to one switch (the command switch) and enabling the switch as the command switch
3. Starting Cluster Builder and adding the candidate switches to the cluster

After the cluster is formed, you can access all switches in the cluster by entering the IP address of the command switch into the browser **Location** field (Netscape Communicator) or **Address** field (Internet Explorer).

## Enabling the Command Switch

You enable the command-switch functionality through the Switch Manager or through the CLI. Before you enable a switch as a command switch, see the [“Command Switch Requirements” section on page 3-3](#) to ensure that the switch meets all the requirements.

Follow these steps to enable the switch as a command switch by using Visual Switch Manager (VSM):

- 
- |               |                                                                                                                         |
|---------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Enter the switch IP address in your browser, and press <b>Return</b> . The Cisco Access Page displays.                  |
| <b>Step 2</b> | Click <b>Cluster Management Suite or Visual Switch Manager</b> on the Cisco Access Page. The switch home page displays. |
| <b>Step 3</b> | Select <b>Cluster &gt; Cluster Command Configuration</b> from the menu bar.                                             |
| <b>Step 4</b> | Select <b>Enable</b> on the Cluster Configuration window. You can use up to 31 characters to name your cluster.         |
-

After you have enabled the command switch, select **Cluster > Cluster Builder** to begin building your cluster. To enable a switch as the command switch by using the command-line interface (CLI), see the “[CLI: Creating a Cluster](#)” section on page 3-8.

## Automatically Discovering Cluster Candidates

Cluster Builder uses the CDP to discover candidate switches that can be added to a cluster. By using CDP, a switch can automatically discover switches in star or cascaded topologies that are up to three CDP-hops away from the edge of the cluster. You can configure the command switch to discover switches up to seven CDP-hops away.

When an edge device that does not support CDP is connected to the command switch, CDP can still discover the candidate switches that are attached to it. When a switch that does support CDP but does not support clustering is connected to the command switch, the cluster is unable to discover candidates that are attached to it. For example, Cluster Builder cannot create a cluster that includes candidates that are connected to a Catalyst 5000 series or 6000 switch connected to the command switch.

When Cluster Builder starts, it automatically prompts you to create a cluster by adding qualified candidates, as shown in [Figure 3-2](#). The Suggested Candidate window lists each candidate switch with its device type, MAC address, and the switch through which it is connected to the cluster. When new switches are added to the topology, Cluster Builder prompts you the next time it starts to add the latest candidate to the cluster. The Suggested Candidate window does not display after the number of switches in the cluster has reached the maximum of 16.

By default, the suggested candidates are highlighted in the Suggested Candidates window, but you can select one or more switches as long as the number of switches selected does not exceed 16. You can accept the suggested candidates or not. If you do not accept the suggested candidates, none of the switches are added.



### Note

---

You can always select one or more candidates in Cluster Builder and select **Add to Cluster** to add them to the cluster.

---

When you accept the suggested candidates, enter the password of the candidate switch if one has been defined. If no password has been defined, click **OK** to add the switch to the cluster with no password. If you enter a password that does not

match the password defined for the candidate, or if the switch does not have a password, it does not look at the password field, and the candidate is not added to the cluster. In all cases, once a candidate switch joins a cluster, it inherits the command-switch password. For more information on setting passwords, see the [“Changes to Passwords” section on page 3-11](#).

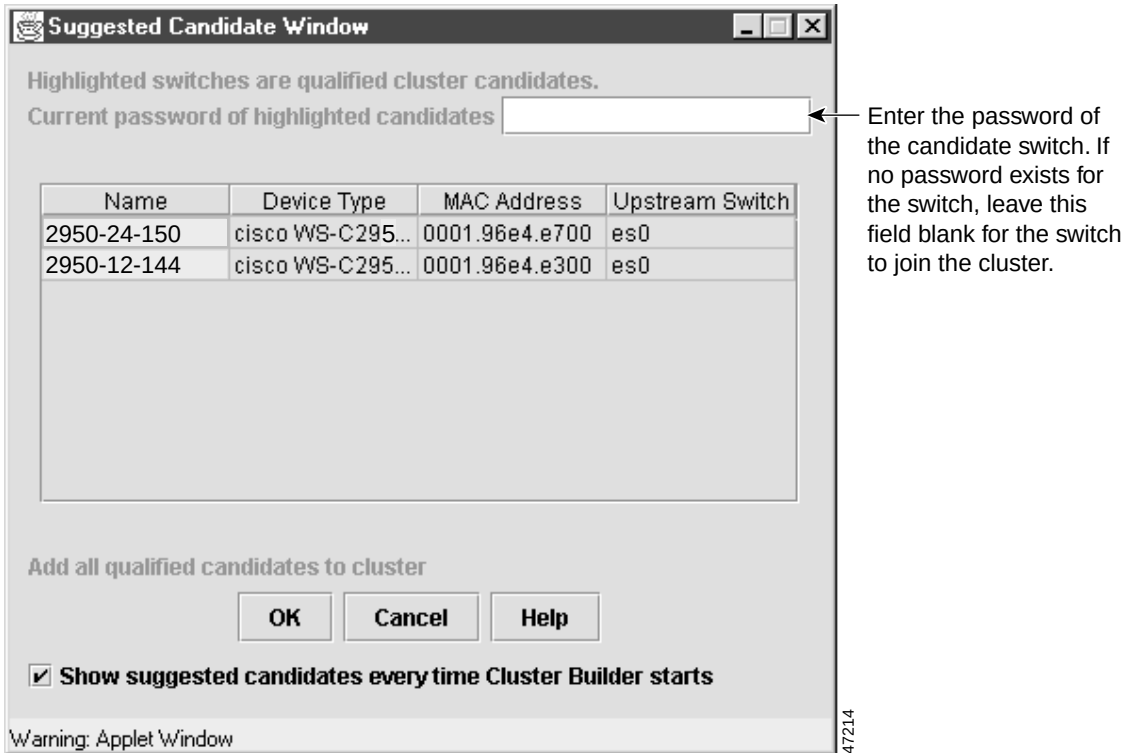
**Note**

---

The Suggested Candidates window displays prequalified candidates whether or not they are in the same management VLAN as the command switch. If you enter the password for a candidate in a different management VLAN than the cluster and click **OK**, this switch is not added to the cluster. It appears as a candidate switch in Cluster Builder. For information on how to change the management VLAN, see the [“Understanding Management VLAN Changes” section on page 3-4](#).

---

You can set Cluster Builder to not automatically display suggested candidates. For more information, see the [“Changing User Settings” section on page 3-31](#).

**Figure 3-2 Suggested Candidate Window**

## CLI: Creating a Cluster

This procedure assumes that the candidate switches and the command switch are connected through ports that belong to the same management VLAN. The [“Changing the Management VLAN” section on page 3-34](#) describes the characteristics of the management VLAN.

Beginning in privileged EXEC mode on the command switch, follow these steps to enable the command switch and add candidate switches to the cluster:

|        | Command                                                                                          | Purpose                                                                                                                                                                                                                                                                                            |
|--------|--------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>                                                                        | Enter global configuration mode.                                                                                                                                                                                                                                                                   |
| Step 2 | <b>cluster enable</b> <i>name</i>                                                                | Enable the command switch and name the cluster (up to 31 characters).                                                                                                                                                                                                                              |
| Step 3 | <b>end</b>                                                                                       | Return to privileged EXEC mode.                                                                                                                                                                                                                                                                    |
| Step 4 | <b>show cluster candidates</b>                                                                   | Display a list of candidates.                                                                                                                                                                                                                                                                      |
| Step 5 | <b>show cluster members</b>                                                                      | Display a list of current cluster members.                                                                                                                                                                                                                                                         |
| Step 6 | <b>configure terminal</b>                                                                        | Enter global configuration mode.                                                                                                                                                                                                                                                                   |
| Step 7 | <b>cluster member</b> <i>n</i> <b>mac-address</b> <i>hw-addr</i> <b>password</b> <i>password</i> | Add candidates to the cluster.<br><br>Assign a unique number from 1 to 15 for <i>n</i> . Do not use any switch number (SN) that appears in the <b>show cluster members</b> display. Enter the candidate switch MAC address, which can be obtained from the <b>show cluster candidates</b> display. |
| Step 8 | <b>end</b>                                                                                       | Return to privileged EXEC mode.                                                                                                                                                                                                                                                                    |
| Step 9 | <b>show cluster members</b>                                                                      | Display the status of the cluster.                                                                                                                                                                                                                                                                 |

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## When a Cluster is Created

When a cluster is created, Network Address Translation (NAT) commands are added to the configuration file of the command switch. Do not remove these commands. The command switch also automatically makes configuration changes to the member switch host name, password, and SNMP community string.

## Changes to the Host Name

If you did not assign a host name to a member switch, the command switch appends a unique member number to its own host name and assigns it sequentially to the switch when it joins the cluster. The number indicates the order in which the switch was added to the cluster. For example, a command switch named *eng-cluster* could name cluster member 5 *eng-cluster-5*.

If you did not assign a host name to the command switch, it keeps the default host name of *Switch*.

If you assigned a host name to a member switch, it retains that name when it joins the cluster. A host name is also retained even after removing the switch from the cluster.

However, if your switch was part of a cluster, received its host name from the command switch, was removed and then added back to a new cluster, its host name (such as *eng-cluster-5*) is not overwritten with the new version of the command switch host name.

## Changes to the SNMP Community Strings

The following SNMP community strings are added to a member switch when it joins a cluster:

- `commander-readonly-community-string@esN`, where N is the member-switch number.
- `commander-readwrite-community-string@esN`, where N is the member-switch number.

If the command switch has multiple read-only or read-write community strings, only the first read-only and read-write strings are propagated to the member switch.

Catalyst 2950, 2900 XL, and 3500 XL switches support an unlimited number of community strings and string lengths.

The Catalyst 1900 and 2820 switches support up to four read-only and four read-write community strings; each string contains up to 32 characters. When these switches join the cluster, the first read-only and read-write community string on the command switch is propagated and overwrites the fourth read-only and read-write community string on the member switches. To support the 32-character string-length limitation on the Catalyst 1900 and 2820 switches, the

command-switch community strings are truncated to 27 characters when propagating them to these switches, and the @esN (where N refers to the member switch number and can be up to two digits) is appended to them.

For more information about configuring community strings through Cluster Manager, see the [“Configuring SNMP” section on page 4-41](#).

## Changes to Passwords

The member switch inherits the command-switch enable-secret or enable password when it joins the cluster and retains it when it leaves the cluster. If no command-switch password is configured, the member switch inherits a null password. Member switches only inherit the command-switch password privilege level 15.

However, certain caveats apply to Catalyst 1900 and 2820 switches as cluster members. Their passwords and privilege levels are altered in the following ways:

- Password length
  - If the command-switch enable password is longer than 8 characters, the member-switch enable password is truncated to 8 characters.
  - If the command-switch enable password is between 1 and 8 characters inclusive, the member-switch enable password will be the same as the command switch password. (Though the password length for Catalyst 1900 and 2820 switches is from 4 to 8 characters, the length is only checked when the password is configured from the menu console or with the CLI.)
  - Both the command switch and member switch support up to 25 characters (52 characters encrypted) in the enable secret password.

- Privilege level

The command switch supports up to 15 privilege levels. Catalyst 1900 and 2820 member switches support only levels 1 and 15.

- Command-switch privilege levels 1 to 14 map to level 1 on the member switch.
- Command-switch privilege level 15 maps to level 15 on the member switch.

## Adding and Removing Member Switches

You can use the network map in Cluster Builder ([Figure 3-3](#)) to add a switch or switches to a cluster. Clustered switches have green labels, and candidates have blue labels. To add a single switch to a cluster, right-click the candidate, and click **Add to Cluster** from the pop-up menu. If the candidate is in a different management VLAN than the command switch, a message is displayed indicating that this candidate is unreachable, and you will not be able to add it to the cluster.

To add several switches to a cluster, press **Ctrl**, and left-click the candidates you want to add. The candidates are added if they all have the same password. If any of the candidates cannot be added, Cluster Builder displays a message explaining which candidates were not added and why.

You can add a candidate to a cluster if no more than 16 switches are in the cluster; otherwise, you must remove a member before adding a new one. If a password has been configured on the switch, you are prompted to enter.

**Note**

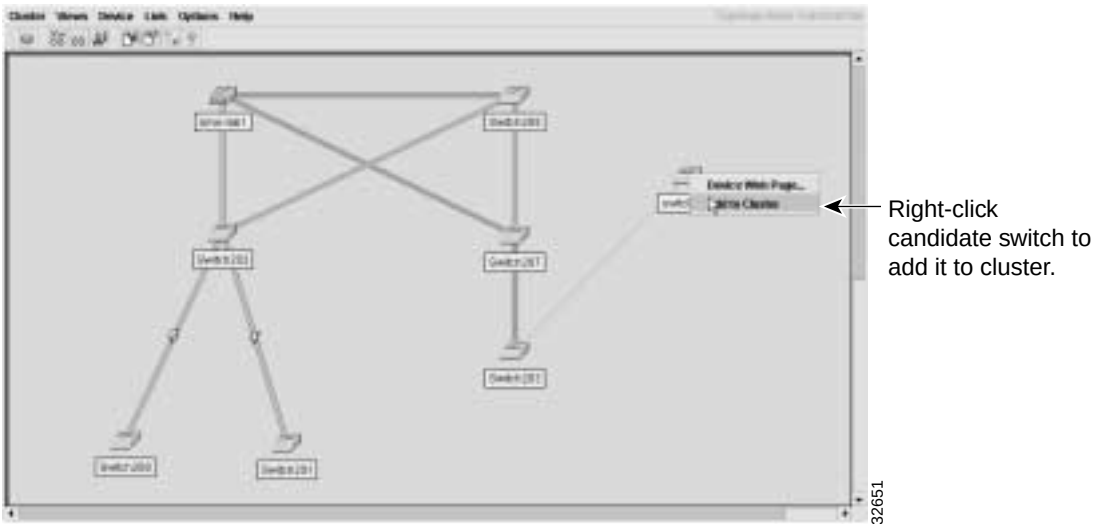
---

The Add to Cluster option is disabled when the number of switches in the cluster reaches 16.

---

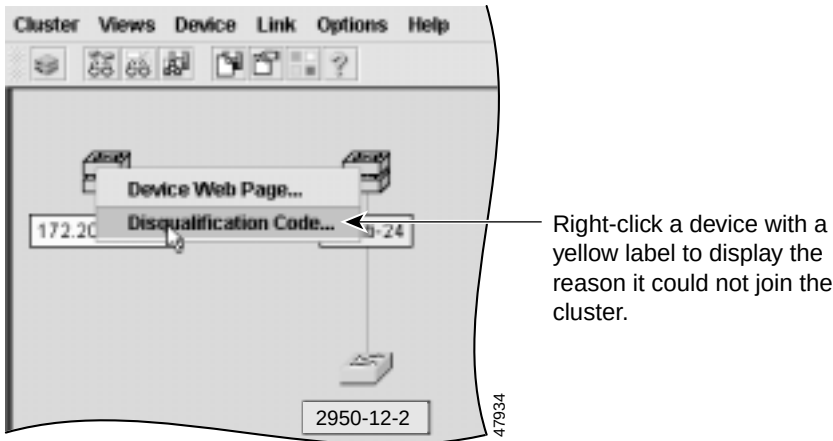
To remove a member switch, right-click it, and select **Remove from Cluster** from the pop-up menu. The switch retains the password configured for it when it leaves the cluster. You can also use the CLI to remove a member switch, as described in the [“CLI: Removing a Member from a Cluster”](#) section on page 3-16.



**Figure 3-3 Cluster Builder**

## Determining Why a Switch Is Not Added to a Cluster

If a switch does not become part of the cluster, you can learn why by selecting **Views > Toggle View** from the menu bar in Cluster Builder. Cluster View displays the cluster as a double-switch icon and shows connections to devices outside of the cluster (Figure 3-4). Right-click the device (yellow label), and select **Disqualification Code** to display the reason it did not join the cluster.

**Figure 3-4 Cluster View**

## CLI: Adding a Member to a Cluster

You can use the **cluster setup** command to add members to an existing cluster or to create a cluster. This command generates a script that proposes configuration changes and prompts you to approve or disapprove them. Enter this command from a switch that is enabled as a command switch.



### Note

Only candidate switches that are one hop away and have not been assigned an IP address are displayed by this command. You can display all valid candidates by using the **show cluster candidates** command, and you can display all cluster members by using the **show cluster members** command.

Beginning in privileged EXEC mode on a command switch, follow these steps to add a member switch to a cluster:

|        | Command                                                                                                                                                                                                                 | Purpose                                                                                                                                                                                                                                                                                                                                              |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>cluster setup</b>                                                                                                                                                                                                    | Start the setup script. You can end the script at any time by entering <b>ctrl-c</b> .                                                                                                                                                                                                                                                               |
| Step 2 | <b>Continue with cluster configuration dialog? [yes/no]:</b><br><b>yes</b><br><br><b>The following configuration command script was created:</b><br><b>cluster member <i>n</i> mac-address</b><br><b><i>hw-addr</i></b> | The current cluster members and candidates are displayed. When prompted by the script, enter <b>yes</b> to accept the proposed cluster configuration or <b>no</b> to reject it.<br><br>If you enter <b>yes</b> , the script displays candidates that have been added to the cluster. If you enter <b>no</b> , the <b>cluster setup</b> command ends. |
| Step 3 | <b>Use this configuration? [yes/no]:</b><br><b>yes</b>                                                                                                                                                                  | Enter <b>yes</b> to accept the proposed configuration or <b>no</b> to reject it.<br><br>If you enter <b>yes</b> , the candidate switches are added to the cluster. If you enter <b>no</b> , the <b>cluster setup</b> command ends.                                                                                                                   |
| Step 4 | <b>end</b>                                                                                                                                                                                                              | Return to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                      |
| Step 5 | <b>show cluster members</b>                                                                                                                                                                                             | Verify that all members have been added to the cluster.                                                                                                                                                                                                                                                                                              |

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## CLI: Removing a Member from a Cluster

You remove a cluster member by entering commands on the command switch.

Beginning in privileged EXEC mode on the command switch, follow these steps to remove a member switch from the cluster:

|        | Command                           | Purpose                                                                                                         |
|--------|-----------------------------------|-----------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>show cluster members</b>       | Display the status of the cluster, and note the MAC address and member number of the switch you want to remove. |
| Step 2 | <b>configure terminal</b>         | Enter global configuration mode.                                                                                |
| Step 3 | <b>no cluster member <i>n</i></b> | Remove the switch from the cluster, where <i>n</i> is the switch member number.                                 |
| Step 4 | <b>end</b>                        | Return to privileged EXEC mode.                                                                                 |
| Step 5 | <b>show cluster members</b>       | Display the status of the new cluster.                                                                          |

You can remove a member by entering commands on the member itself, but the member is not entirely removed from the cluster until you also enter commands on the cluster command switch. A member switch that is removed by entering commands only on the member switch is considered by the command switch to be *down* until it is explicitly removed on the command switch.

Beginning in privileged EXEC mode on a Catalyst 2950, 2900 XL, or 3500 XL member switch, follow these steps to remove it from a cluster:

|        | Command                             | Purpose                                                         |
|--------|-------------------------------------|-----------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>           | On the member switch, enter global configuration mode.          |
| Step 2 | <b>no cluster commander-address</b> | Remove the member switch from the cluster.                      |
| Step 3 | <b>end</b>                          | Return to privileged EXEC mode.                                 |
| Step 4 | <b>show cluster</b>                 | Verify that the member switch is no longer part of the cluster. |

|        | Command                           | Purpose                                                                                                                                |
|--------|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| Step 5 | <b>show cluster members</b>       | On the command switch, display the status of the cluster, and note the MAC address and switch number of the switch you want to remove. |
| Step 6 | <b>configure terminal</b>         | Enter global configuration mode.                                                                                                       |
| Step 7 | <b>no cluster member <i>n</i></b> | Remove the switch from the cluster.                                                                                                    |
| Step 8 | <b>end</b>                        | Return to privileged EXEC mode.                                                                                                        |
| Step 9 | <b>show cluster members</b>       | Display the status of the new cluster.                                                                                                 |

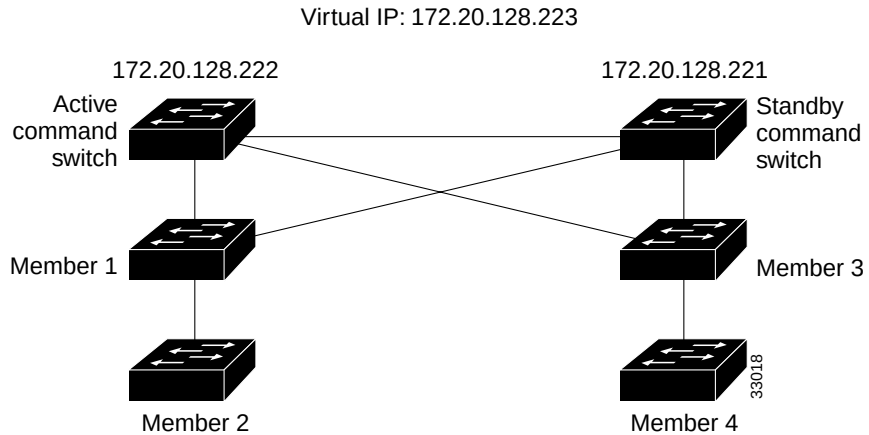
For information on how to remove Catalyst 1900 or 2820 member switches, refer to the *Catalyst 1900 Series Installation and Configuration Guide* or the *Catalyst 2820 Series Installation and Configuration Guide*.

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## Building a Redundant Cluster

Because a cluster command switch manages the forwarding of all configuration information to cluster members, a redundant command switch is necessary to take over if the command switch fails. Cisco IOS Release 12.0(5)WC(1) supports a version of the HSRP so that you can configure a *standby group* of Catalyst 2950, 2900 XL, or 3500 XL switches. When this standby group is *bound* to the cluster, one of the switches acts as a standby command switch that becomes active when the command switch fails. The [“Understanding HSRP”](#) section on page 3-18 describes how the protocol works.

Redundant cabling is also required for a standby switch to automatically take over when a command switch fails. [Figure 3-5](#) shows a network cabled to allow the standby switch to maintain management contact with the member switches if the cluster command switch fails. Spanning Tree Protocol prevents the loops in such a configuration from reducing performance.

**Figure 3-5 Redundant Cabling to Support HSRP**

## Understanding HSRP

To build a redundant cluster, you use HSRP to configure a stand-by group that contains a cluster command switch and one or more eligible member switches. The standby group is configured with a unique virtual IP address. When the standby group is bound on the command switch, the command switch receives member traffic destined for the virtual IP address.

To manage the redundant cluster, access the command switch through the virtual IP address and not the command-switch IP address. If HSRP is enabled and you use the command-switch IP address, you can be prompted a second time for a password when you move between Cluster Builder and VSM.

Other switches in the standby group are candidates to become the standby command switch and are ranked according to a set of user-defined priorities. The member switch with the highest priority in the group is the standby command switch. To ensure that the standby command switch can take over the cluster if the command switch fails, the command switch continually forwards cluster configuration information to the standby command switch.

**Note**

The command switch forwards cluster configuration information to the standby switch but not device-configuration information. The standby command switch is informed of new cluster members but not the configuration of any given switch.

If the command switch fails, the standby command switch assumes ownership of the virtual IP address and MAC address and begins acting as the command switch. The remaining switches in the group compare their assigned priorities to determine the new standby command switch. To configure an HSRP standby group, see the [“Configuring a Cluster Standby Group” section on page 3-19](#).

If a standby switch replaces a command switch and the command switch becomes active again, the command switch resumes its role as the active command switch. An automatic recovery procedure can add cluster members that were added to the cluster while the command switch was down.

## Recovering from a Failed Command Switch without HSRP

If a command switch fails and no standby command switch is configured, member switches continue forwarding among themselves, and they retain the ability to be managed through normal standalone means. You can configure member switches through the console-port CLI, and they can be managed through SNMP, HTML, and Telnet after you assign an IP address to them.

The password you enter when you log into the command switch gives you access to member switches. If the command switch fails and there is no standby command switch, you can use the command-switch password to recover. For more information, see [“Recovering from a Command Switch Failure” section on page 7-8](#).

## Configuring a Cluster Standby Group

This section describes how to create a standby group and bind it to a cluster, how to add and remove members from a standby group, and how to remove a standby group from the network.

Use the Standby Command Configuration window ([Figure 3-6](#)) to create a standby group. When an active command switch fails, a new command switch is chosen from this group according to their order in their Selected list in the window.

## Standby Command Switch Requirements

To be eligible to join a standby group, a switch must meet the following requirements:

- It is running Cisco IOS Release 12.0(5)XU or later.
- It has its own IP address.

Any number of eligible switches can belong to a standby group.



### Note

---

Switches running earlier releases of the IOS software can belong to clusters supported by HSRP but cannot belong to a standby group.

---

For redundancy, we also recommend that a switch belonging to a standby group have the following characteristics:

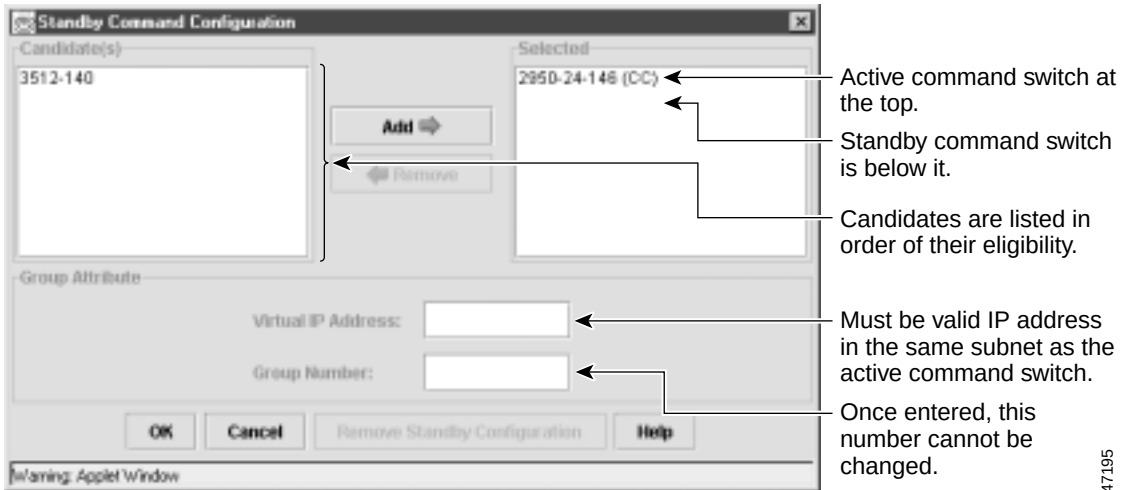
- It is a member of a cluster.
- It is cabled so that connectivity to cluster members is maintained even if the command switch fails.

## Using the Standby Configuration Window

You create a standby group by moving candidates from the Candidates list to the Selected list in the Standby Command Configuration window ([Figure 3-6](#)). Eligible switches are listed in the Candidates list according to an eligibility ranking. Switches are ranked first by the number of links they have and second by the speed of the switch. If switches have the same number of links and speed, they are listed alphabetically.

When you add a switch to the standby group, you can configure the priority of group members by using the **Add** and **Remove** buttons. The command switch has the highest priority and is always at the top of the list. The standby switch is below the command switch, and the priority of the other switches is represented by their place in the list. The last switch in the list has the lowest priority.



**Figure 3-6 Standby Command Configuration**

47195

The following abbreviations are appended to the switch host names in the Selected list to indicate their status in the standby group:

- AC Active command switch
- SC Standby command switch
- PC Passive command switch (member of the standby group but is not the standby command switch)
- CC Command switch when HSRP is disabled

The virtual IP address (VIP) must be in the same subnet as the IP addresses of the switches, and the group number must be unique within the IP subnet. It can be from 0 to 255, and the default is 0. The VIP should be different from the commander IP address to avoid duplicate IP addresses.

The Standby Command Configuration window uses default values for the **preempt** and **name** commands that you can explicitly set by using the CLI. If you use this window to create the HSRP group, all switches in the group have the preempt command enabled, and the name for the group is *clustername\_standby*.

## CLI: Creating a Standby Group

There are two steps to configuring a standby group through the CLI:

1. Entering the name, number, and virtual IP address of the HSRP group on each switch in the group, including the command switch.
2. Binding the HSRP group to the cluster by entering the redundancy-enable command on the cluster command switch.

Follow these guidelines when you configure a standby group by using the CLI:

- Configure one HSRP group per cluster.
- Assign the unique virtual IP address to every switch in the group.
- Assign the unique name to every switch in the group.
- Assign the standby priority to each switch in relation to the active command switch. That is, the active command switch has the highest priority, the switch with the most redundant connectivity has the next highest priority, and so on.
- Enter the preempt command on each switch to ensure that the priority is maintained.

Beginning in privileged EXEC mode on the command switch, follow these steps to create the HSRP group and bind it to the command switch:

|        | Command                             | Purpose                                                                                                                                                                     |
|--------|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>           | Enter global configuration mode.                                                                                                                                            |
| Step 2 | <b>interface vlan1</b>              | Set the switch to configure the management interface in VLAN 1.                                                                                                             |
| Step 3 | <b>standby number ip ip_address</b> | Create the standby group, and give it a number and virtual IP address. The group number must be unique within the IP subnet. It can be from 0 to 255, and the default is 0. |

|         | Command                                                      | Purpose                                                                                                                                                                                                 |
|---------|--------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 4  | <b>standby</b> <i>number</i> <b>name</b> <i>name</i>         | Give the standby group a name. This name is used to bind the group to the command switch. The name can be a string up to 32 characters long.                                                            |
| Step 5  | <b>standby</b> <i>number</i> <b>priority</b> <i>priority</i> | Set the priority of the switch to a number between 0 and 255. Assign the highest priority to the command switch. The default priority is 100.                                                           |
| Step 6  | <b>standby</b> <i>number</i> <b>preempt</b>                  | Set the standby group to always maintain the priority ranking, even when the command switch fails and becomes active again.                                                                             |
| Step 7  | <b>end</b>                                                   | Return to privileged EXEC mode.                                                                                                                                                                         |
| Step 8  | <b>show running-config</b>                                   | Verify the creation of the standby group.                                                                                                                                                               |
| Step 9  |                                                              | Repeat Steps 1 through 6 on each switch eligible to belong to the group. Configure the priority to ensure that the best-suited standby switch has the highest priority after the active command switch. |
| Step 10 | <b>configure terminal</b>                                    | After all eligible switches have been added to the group, return to the command switch CLI, and enter global configuration mode.                                                                        |
| Step 11 | <b>cluster standby-group</b> <i>name</i>                     | Enable command-switch redundancy for the cluster by entering the name of the standby group you created in Step 4.                                                                                       |
| Step 12 |                                                              | Begin to use the virtual IP address that you entered in Step 3 as the means to manage the cluster.                                                                                                      |

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## CLI: Adding Member Switches to a Standby Group

Member switches must have an IP address and be running Cisco IOS Release 12.0(5)XU or later before they can be added to an existing HSRP group. Beginning in privileged EXEC mode on the command switch, follow these steps to add the switch to the HSRP group:

|         | Command                                 | Purpose                                                                                                                                                                                                                                        |
|---------|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1  | <b>configure terminal</b>               | Enter global configuration mode.                                                                                                                                                                                                               |
| Step 2  | <b>interface vlan1</b>                  | Set the switch to configure the management interface in VLAN 1.                                                                                                                                                                                |
| Step 3  | <b>show cluster</b>                     | Display the HSRP group number to which the cluster is bound.                                                                                                                                                                                   |
| Step 4  | <b>show standby</b>                     | Display the information defined for the existing HSRP group, and note the virtual IP address, name, and priority.                                                                                                                              |
| Step 5  | <b>show cluster members</b>             | Display the members that are part of the cluster. From the display, get the number of the member switch that you want to add to the group. The member number is listed in the SN column of the display. You need the member number for Step 6. |
| Step 6  | <b>rcommand n</b>                       | Access the CLI for the member switch that you want to add to the group.<br><br>For <i>n</i> , enter the switch number that you obtained in Step 5.                                                                                             |
| Step 7  | <b>configure terminal</b>               | On the member switch, enter global configuration mode.                                                                                                                                                                                         |
| Step 8  | <b>standby number ip ip_address</b>     | Enter the group number and the virtual IP address.                                                                                                                                                                                             |
| Step 9  | <b>standby number name name</b>         | Enter the HSRP group number and name.                                                                                                                                                                                                          |
| Step 10 | <b>standby number priority priority</b> | Set the priority of the switch to a number between 0 and 255.                                                                                                                                                                                  |

|         | Command                              | Purpose                                                                                                                     |
|---------|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| Step 11 | <b>standby <i>number</i> preempt</b> | Set the standby group to always maintain the priority ranking, even when the command switch fails and becomes active again. |
| Step 12 | <b>end</b>                           | Return to privileged EXEC mode.                                                                                             |
| Step 13 | <b>show cluster members</b>          | Verify that the member was added to the cluster.                                                                            |

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## CLI: Removing a Switch from a Standby Group

You can remove standby switches from a standby group, but you cannot remove an active command switch from a standby group. Beginning in privileged EXEC mode on the command switch, follow these steps to remove a switch from the HSRP group:

|        | Command                       | Purpose                                                                                                                                                                                                                                             |
|--------|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>     | Enter global configuration mode.                                                                                                                                                                                                                    |
| Step 2 | <b>interface <i>vlan1</i></b> | Set the switch to configure the management interface in VLAN 1.                                                                                                                                                                                     |
| Step 3 | <b>show cluster</b>           | Display the standby group number to which the cluster is bound. Note the number.                                                                                                                                                                    |
| Step 4 | <b>show cluster members</b>   | Display the members that are part of the cluster. From the display, get the number of the member switch that you want to remove from the group. The member number is listed in the SN column of the display. You need the member number for Step 5. |
| Step 5 | <b>rcommand <i>n</i></b>      | Access the CLI for the member switch you want to remove from the group.<br><br>For <i>n</i> , enter the switch number that you obtained in Step 4.                                                                                                  |

|         | Command                                  | Purpose                                                |
|---------|------------------------------------------|--------------------------------------------------------|
| Step 6  | <b>configure terminal</b>                | Enter global configuration mode.                       |
| Step 7  | <b>no standby <i>number</i> ip</b>       | Use the group number to remove the virtual IP address. |
| Step 8  | <b>no standby <i>number</i> name</b>     | Use the group number to remove the name setting.       |
| Step 9  | <b>no standby <i>number</i> priority</b> | Use the group number to remove the priority setting.   |
| Step 10 | <b>no standby <i>number</i> preempt</b>  | Use the group number to remove the preempt setting.    |

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## CLI: Removing a Standby Group from the Network

You remove a standby group from your network by disabling the standby group on the command switch and entering the **no** version of the HSRP CLI commands on all switches in the HSRP group. When all HSRP parameters have been removed from all the members of the group, including the command switch, the group has been removed from the network.

Beginning in privileged EXEC mode on the command switch, follow these steps to remove a standby group:

|        | Command                              | Purpose                                                                     |
|--------|--------------------------------------|-----------------------------------------------------------------------------|
| Step 1 | <b>show cluster</b>                  | Display the standby group number.                                           |
| Step 2 | <b>configure terminal</b>            | Enter global configuration mode.                                            |
| Step 3 | <b>no cluster standby-group</b>      | Unbind the command switch from the standby group.                           |
| Step 4 | <b>no standby <i>number</i> ip</b>   | Use the group number to remove the virtual IP address of the standby group. |
| Step 5 | <b>no standby <i>number</i> name</b> | Use the group number to remove the name setting.                            |

|        | Command                                  | Purpose                                                                                                                                                                                |
|--------|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 6 | <b>no standby <i>number</i> priority</b> | Use the group number to remove the priority setting.                                                                                                                                   |
| Step 7 | <b>no standby <i>number</i> preempt</b>  | Use the group number to remove the preempt setting.                                                                                                                                    |
| Step 8 | <b>show cluster members</b>              | Display the members that are part of the cluster. From the display, get the number of the switch that you want to remove from the group. You need the member number for Step 9.        |
| Step 9 | <b>rcommand <i>n</i></b>                 | Access the CLI for each switch in the group, enter global configuration mode, and repeat Steps 4 through 7.<br><br>For <i>n</i> , enter the switch number that you obtained in Step 8. |

**Note**

After the last switch has been removed from the standby group, start accessing the cluster by using the IP address of the command switch.

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## Managing Switch Clusters

This section describes how to perform tasks on switch clusters. Cluster members could be Catalyst 1900, 2820, 2950, 2900 XL, or 3500 XL switches. These management tasks operate on all switches in the cluster and are distinct from configuring individual switches. For information on managing individual devices, see [Chapter 4, “Managing Switches.”](#)

This section describes how to perform the following tasks:

- Accessing CMS
- Configuring initial cluster settings
- Saving configuration changes

- Displaying an inventory of cluster switches
- Monitoring and configuring ports
- Changing the management VLAN for a cluster
- Displaying link information
- Displaying VLAN membership information
- Upgrading the switch software on all switches in the cluster
- Enabling and configuring SNMP

## Accessing the Cluster Management Suite

If you have not already configured your browser for CMS, refer to the *Release Notes for the Catalyst 2950 Cisco IOS Release 12.0(5)WC(1)* for detailed instructions on configuring the browsers.

When you enter the switch IP address in the browser **Location** field (Netscape Communicator) or **Address** field (Internet Explorer), the Cisco Systems Access page ([Figure 3-7](#)) is displayed. Click **Cluster Management Suite or Visual Switch Manager**. Cluster Builder or Cluster Manager displays ([Figure 3-8](#)).



Figure 3-7 Cisco Systems Access Page

**Cisco Systems**

Accessing Cisco WS-C2950-24 "2950-24-146"

[Cluster Management Suite or Virtual Switch Manager](#) ← Click here to display CMS or VSM.

[Telnet - To the Switch.](#) ← Click here to open a Telnet session to the switch.

[Show interfaces](#) - Display the status of the interfaces.

[Show diagnostic log](#) - Display the diagnostic log.

[Web Console](#) - HTML access to the command line interface at level [0](#), [1](#), [2](#), [3](#), [4](#), [5](#), [6](#), [7](#), [8](#), [9](#), [10](#), [11](#), [12](#), [13](#), [14](#), [15](#)

[Show tech support](#) - Display information commonly needed by tech support. ← Click here to display the switch configuration file and other troubleshooting information.

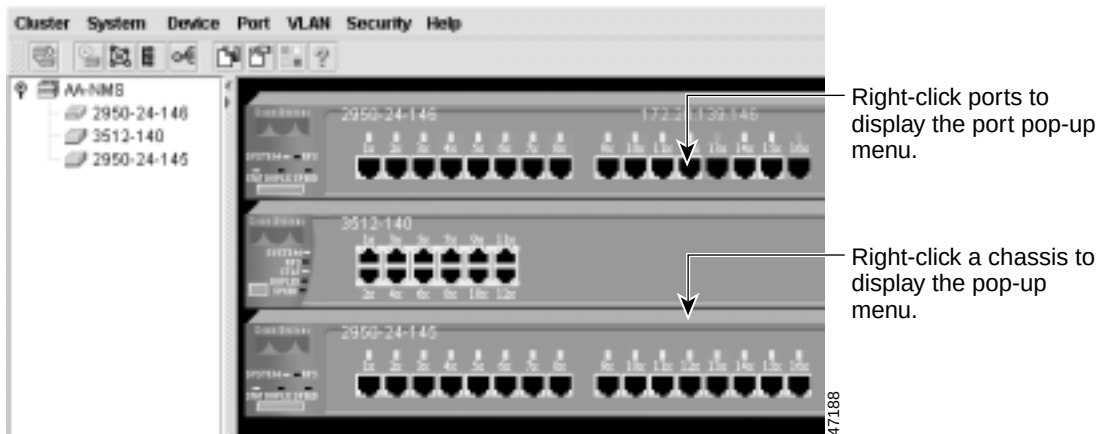
**Help resources**

1. [CCO at www.cisco.com](#) - Cisco Connection Online, including the Technical Assistance Center (TAC).
2. [tac@cisco.com](#) - e-mail the TAC.
3. 1-800-553-2447 or +1-408-526-7209 - phone the TAC.
4. [cc.html@cisco.com](#) - e-mail the HTML interface development group.

← How to contact Cisco Systems.

47191

After you have created a cluster, you can use Cluster Manager to monitor and configure the cluster switches. Figure 3-8 shows a cluster displayed in Cluster Manager. The switch software updates the LEDs displayed on these images in real time, making the images displayed by Cluster Manager as informative as the switch LEDs themselves. You can also use Cluster Builder and Cluster View to manage your cluster.

**Figure 3-8 Cluster Manager**

## Configuring Initial Cluster Settings

This section describes how to customize the CMS environment to meet your needs.

## Arranging and Saving the Network Map

You can reposition devices in Cluster Builder and Cluster View and save this information. Before arranging and saving the network map, make sure that the command switch discovered all the devices and that you have added them to the cluster.

You arrange the layout by clicking and holding the left mouse-button on a device and dragging it to a new location on the map. Select **Options > Save Layout** from the menu bar to save the arrangement displayed by Cluster Builder and Cluster View.

If the topology did not change, the saved version of the network map displays the next time you start Cluster Builder or Cluster View. If a topology change occurs, you can arrange the devices and save the map again.

## Changing User Settings

Select **Cluster > User Settings** from the menu bar in Cluster View, Cluster Builder, or Cluster Manager to change the parameters described in the following list. The user settings are automatically saved in permanent storage on the command switch.

- Cluster Builder and Cluster Manager polling interval—Select the number of seconds the switch waits before polling the switch for new cluster and port information by clicking on the slide bar and moving it to the left or right. Lowering the polling interval can be useful when you are changing or testing cluster switches. The default is 120 seconds.

Reload the page for the new setting to take effect.



### Tips

---

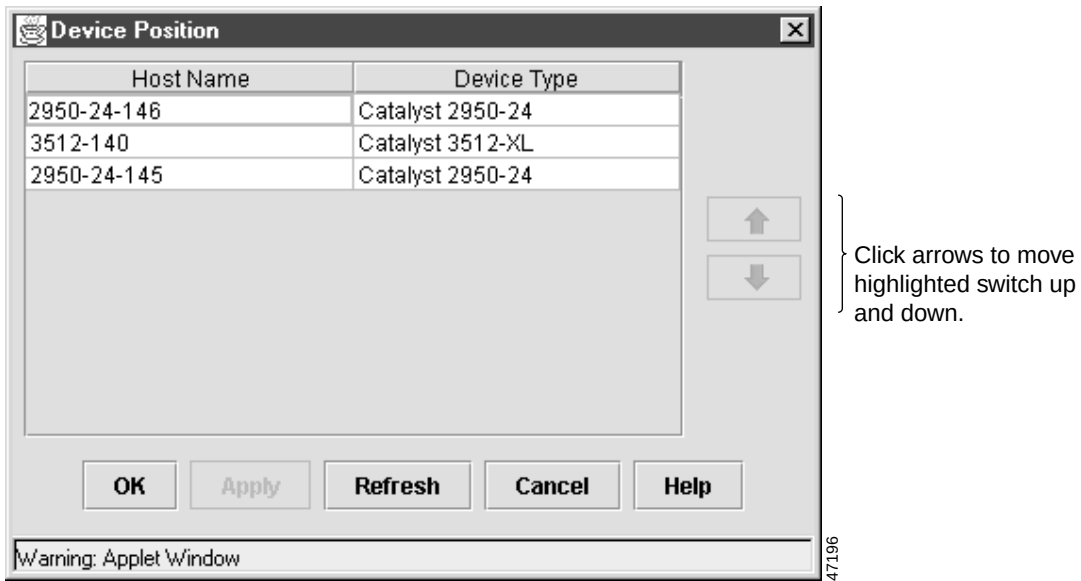
A long polling interval reduces the number of requests made on the command switch, and topology updates are not reported as frequently. A short polling interval has the opposite effect. We recommend that you use a short interval only for troubleshooting or while building a cluster.

---

- Link and device graph polling interval—Select the number of seconds the switch waits before the application polls it for new graph information by clicking on the slide bar and moving it to the left or right. The default is 24 seconds. Reload the page for the new setting to take effect.
- Show the splash screen when the Cluster Management Suite starts—Select **Show Splash Screen** at startup to always see the splash screen.
- Change the default view—Choose Cluster Manager or Cluster Builder as the default view to display when CMS starts. For example, you might make Cluster Manager the default after the cluster-creation process is complete.

## Rearranging the Order of the Displayed Switches

You can arrange the order in which switches are displayed in Cluster Manager to match the arrangement in your wiring closet. Select **Cluster > Device Position** from the menu bar to display the Device Position window (Figure 3-9). Select a device in the Device Position window, and use the arrows to move it up or down in the list. Click **OK** when you are finished.

**Figure 3-9 Device Position**

## Changing the Host Name

You can change the host name of any switch in the cluster by using Cluster Builder.

To change the host name of a member switch in Cluster Builder, right-click the switch, and select **Host Name Config** from the pop-up menu. Enter a host name of up to 28 characters in the field, and click **OK**. Member switch host names must be unique in the cluster. Do not use a number as the last character in a host name on any switch.

When you change the host name on the command switch, assign a name no longer than 28 characters. Limiting the command switch host name to 28 characters ensures that each member switch host name is unique and viewable in the application. The [“Changes to the Host Name” section on page 3-10](#) describes how the command switch appends a member number to its host name and propagates it to new switches not originally configured with a name when they joined the cluster.

## Saving Configuration Changes

Configuration changes on the Catalyst 2950 switches are not written to Flash memory until you select **System > Save Configuration** in Cluster Manager or **Options > Save Configuration** in Cluster Builder or Cluster View.

As you make cluster configuration changes (except for changes to the network map and in the User Settings window), make sure you periodically save the configuration. The configuration is saved on the command and member switches.

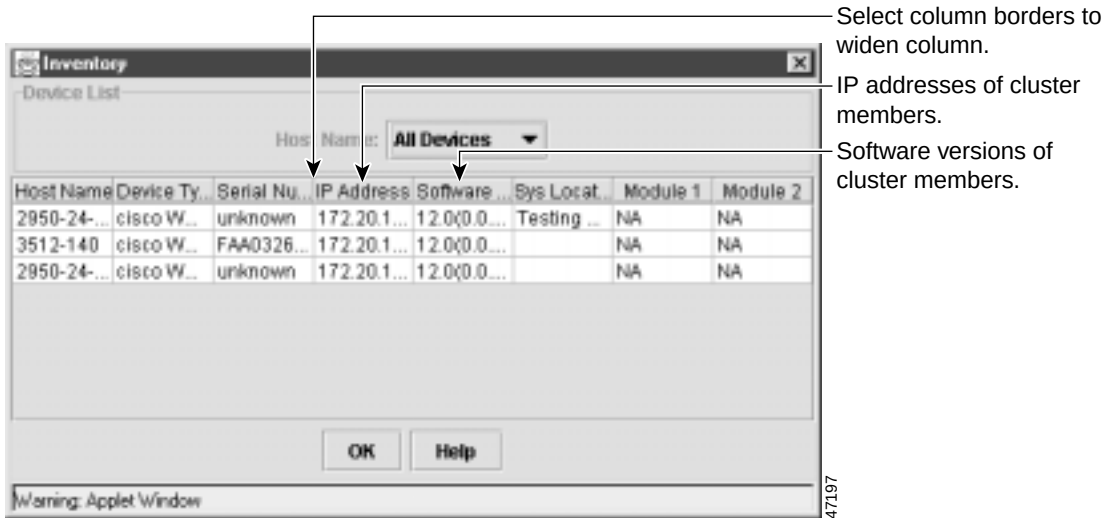
## Displaying an Inventory of Cluster Switches

You can display a summary table of all the switches in a cluster. The cluster inventory contains the following information:

- Cisco model numbers and serial numbers
- IOS version running on the switches
- IP information for the switches
- Location of the switches
- Modules installed in the switches, if applicable

To display the Inventory window ([Figure 3-10](#)), select **System > Inventory**. To display this information for a single switch, select the switch, right-click with the mouse, and select **System > Inventory**.

Figure 3-10 Inventory



## Displaying Link Information

You can see how the cluster members are interconnected by using the Cluster Builder network map. It shows how the switches are connected and the type of connection between each device. Click **Help > Legend** in Cluster Builder to learn the meaning of each icon, link, and color.

To display port-connection information, select **Views > Toggle Labels**. By clicking **Toggle Labels**, you display the port numbers for each end of the link.

## Changing the Management VLAN

Access to all switch management facilities is through the switch IP address, and the switch IP address always belongs to the management VLAN, VLAN 1, by default. This section describes how to configure a cluster to support management connectivity when the management VLAN is other than the default.

## Guidelines for Changing the Management VLAN

The management VLAN has the following characteristics:

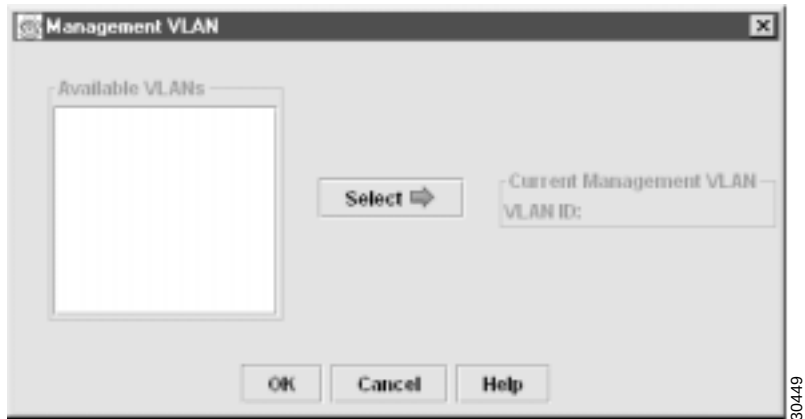
- It is created by the VSM or the CLI on static-access, multi-VLAN, and dynamic-access and trunk ports. You cannot create or remove the management VLAN through SNMP.
- Only one management VLAN can be administratively active at a time.
- With the exception of VLAN 1, the management VLAN can be deleted.
- When created, the management VLAN is administratively down.

Before changing the management VLAN on your switch network, make sure you follow these guidelines:

- The new management VLAN should not have an HSRP standby group configured on it.
- You must be able to move your network management station to a switch port assigned to the same VLAN as the new management VLAN.
- Connectivity through the network must exist from the network management station to all switches involved in the management VLAN change.
- For switches running a version of IOS software that is earlier than Cisco IOS 12.0(5)XP, you cannot change the management VLAN.

## Changing the Management VLAN for a Cluster

To manage switches in a cluster, the port connections among the command, member, and candidate switches must all be in the management VLAN. You can use the VLAN Management window ([Figure 3-11](#)) or the CLI to change the management VLAN of the command and member switches. Any VLAN can serve as the management VLAN as long as there are links between the command switch and the member switches for both the old and the new management VLANs.

**Figure 3-11 Management VLAN**

When you select the new VLAN to be the management VLAN, the IOS software coordinates the change on the member switches to ensure that the cluster continues running without a loss in management connectivity.

If your cluster includes members that are running a software release earlier than Cisco IOS Release 12.0(5)XP, you cannot change the management VLAN of the cluster. If your cluster includes member switches that are running Cisco IOS Release 12.0(5)XP, those members need to have the VLAN changed before using the Management VLAN window. The procedure for changing member switches running Cisco IOS Release 12.0(5)XP is included in the *Cisco IOS Desktop Switching Software Configuration Guide for Catalyst 2900 Series XL and Catalyst 3500 Series XL Cisco IOS Release 12.0(5)XP*.

**Caution**

Changing the management VLAN ends your HTTP or Telnet session. You must restart the HTTP session by entering the switch IP address in the browser **Location** field (Netscape Communicator) or **Address** field (Internet Explorer) or by restarting your CLI session through Telnet. You can change the management VLAN through a console connection without interruption.



## Changing the Management VLAN for a New Switch

For a new switch to be added to a cluster, it must first be connected to a port that belongs to the management VLAN of the cluster. If the cluster is configured with a management VLAN other than the default, the command switch changes the management VLAN for new switches when they are connected to the cluster. In this way, the new switch can exchange CDP messages with the command switch and be proposed as a cluster candidate.

**Note**

For the command switch to change the management VLAN on a new switch, there must be no changes to the switch configuration, and there must be no config.text file.

Because the switch is new and unconfigured, its management VLAN is changed to the cluster management VLAN when it is first added to the cluster. All ports that have an active link at the time of this change become members of the new management VLAN.

## CLI: Changing the Management VLAN Through a Telnet Connection

Before you start, review the [“Guidelines for Changing the Management VLAN” section on page 3-35](#). Beginning in privileged EXEC mode on the command switch, follow these steps to configure the management VLAN interface through a Telnet connection:

|        | Command                                         | Purpose                                                                                                                                                                      |
|--------|-------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>                       | Enter global configuration mode.                                                                                                                                             |
| Step 2 | <b>cluster management-vlan</b><br><i>vlanid</i> | Change the management VLAN for the cluster. This ends your Telnet session. Move the port through which you are connected to the switch to a port in the new management VLAN. |
| Step 3 | <b>show running-config</b>                      | Verify the change.                                                                                                                                                           |

The [“Finding More Information About IOS Commands” section on page 4-1](#) contains the path to the complete IOS documentation.

## Monitoring and Configuring Ports

You can configure one or more ports on the same switch by clicking them from Cluster Manager. You can also configure groups of ports from different switches as a group, and you can display the settings for each port. [Table 3-1](#) describes the parameters that you can monitor and configure.

**Table 3-1** Port Configuration Parameters

| Feature     | Description                                                                                                                                                                                                                                                                                                            |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Status      | Administratively enables or disables the port.                                                                                                                                                                                                                                                                         |
| Description | Displays the description for the port.                                                                                                                                                                                                                                                                                 |
| Duplex      | Sets a port to full-duplex (Full), half-duplex (Half), or autonegotiate (Auto). The default is Auto.<br><br><b>Note</b> The Gigabit Ethernet ports can operate in either half- or full-duplex mode when they are set to 10 or 100 Mbps, but when they are set to 1000 Mbps, they can only operate in full-duplex mode. |
| Speed       | Sets a 10/100 port to 10 Mbps ( <b>10</b> ), 100 Mbps ( <b>100</b> ), or autonegotiate ( <b>Auto</b> ). The default is <b>Auto</b> .<br><br>Sets a 10/100/1000 port to 10 Mbps ( <b>10</b> ), 100 Mbps ( <b>100</b> ), 1000 Mbps ( <b>1000</b> ), or autonegotiate ( <b>Auto</b> ). The default is <b>Auto</b> .       |
| Port Fast   | Sets the port to immediately enter the STP forwarding state and bypass the normal transition from the listening and learning states to the forwarding state.                                                                                                                                                           |

**Table 3-1 Port Configuration Parameters (continued)**

| Feature      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 802.1p       | Assigns a class of service (CoS) priority to the port. CoS values range between zero for lowest-priority and seven for highest-priority. For more information on this parameter, see the <a href="#">“Configuring IEEE 802.1p Class of Service” section on page 5-37</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Flow Control | <p>Enables or disables flow control on Gigabit Ethernet ports. Flow control enables the connected Gigabit Ethernet ports to control traffic rates during congestion. If one port experiences congestion and cannot receive any more traffic, it notifies the other port to stop transmitting until the condition clears.</p> <p>Select <b>Symmetric</b> when you want the local port to perform flow control of the remote port only if the remote port can also perform flow control on the local port.</p> <p>Select <b>Asymmetric</b> when you want the local port to perform flow control on the remote port. For example, if the local port is congested, it notifies the remote port to stop transmitting. This is the default setting.</p> <p>Select <b>Any</b> when the local port can support any level of flow control required by the remote port.</p> <p>Select <b>None</b> to disable flow control on the port.</p> <p>This field is displayed only when a Gigabit Ethernet port is present; it does not apply to a Fast Ethernet port.</p> |

## Monitoring Port Settings

The LEDs on the switch image present the same information as the actual LEDs, but they use colors instead of the on-off methods of the switch front panel.

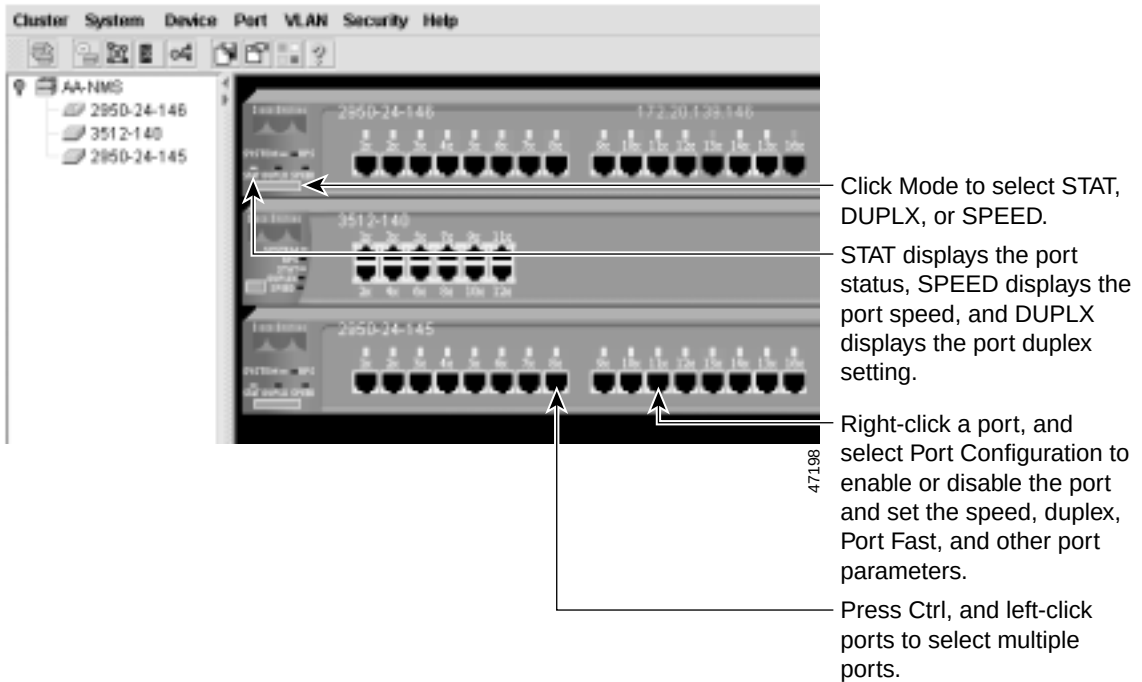
The LEDs above the ports (or the port openings) in [Figure 3-8](#) display the port status (STAT), duplex (DUPLX), or transmission speed (SPEED) of the ports on the switch.



### Note

The UTIL LED is not displayed in Cluster Manager.

Click the Mode button to highlight STAT (status), SPEED (speed), DUPLX (duplex). The port LEDs convey the selected information, and you can select **Help > Legend** to display the color meanings.

**Figure 3-12 Using the Mode Button to Read Switch LEDs**

## Monitoring Other Switch LEDs

The other LEDs function as follows:

- The System LED displays the status of the switch.
- The RPS LED is on when a Cisco RPS is attached. For more information on the RPS, refer to the *Catalyst 2950 Desktop Switch Hardware Installation Guide*.

## Guidelines for Configuring Ports

The Port Configuration window displays the Requested and Actual settings for each port. A port connected to a device that does not support the requested setting or that is not connected to a device can cause the Requested and Actual settings to differ.



### Caution

---

If you reconfigure the port through which you are managing the switch, a Spanning-Tree Protocol (STP) reconfiguration could cause a temporary loss of connectivity.

---

Follow these guidelines when configuring the duplex and speed settings for a switch:

- The Gigabit Ethernet ports can operate in either half- or full-duplex mode when they are set to 10 or 100 Mbps, but when they are set to 1000 Mbps, they can only operate in full-duplex mode.
- If STP is enabled, the switch can take up to 30 seconds to check for loops when a port is reconfigured. The port LED is amber while STP reconfigures.

After you make a change, you can verify the change by clicking the port on the Home page or by using the **Mode** button.

## Connecting to Devices That Do Not Autonegotiate

To connect to a remote 100BaseT device that does not autonegotiate, set the duplex setting to **Full** or **Half**, and set the speed setting to **Auto**. Autonegotiation for the speed setting selects the correct speed even if the attached device does not autonegotiate, but the duplex setting must be explicitly set.

To connect to a remote Gigabit Ethernet device that does not autonegotiate, disable autonegotiation on the local device, and set the duplex and flow control parameters to be compatible with the other device.

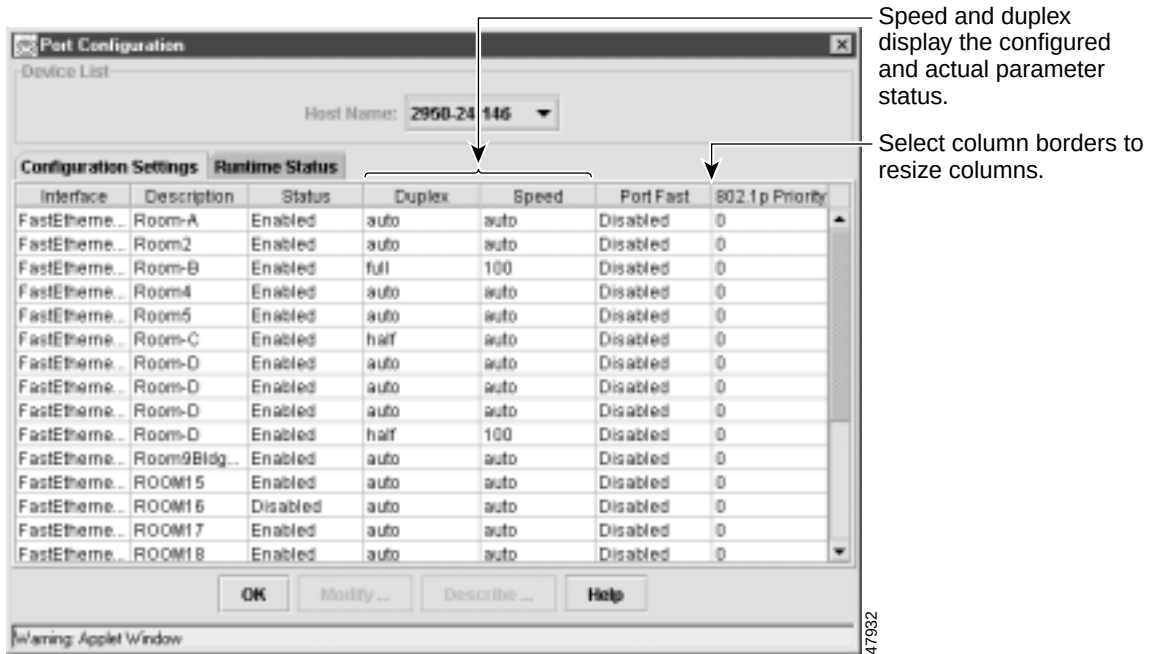
## Configuring Ports

To monitor or reconfigure all the ports of a switch, click the switch, and select **Port > Port Configuration** from the menu bar. The Port Configuration window (Figure 3-13) displays a table with the configured and actual status of each port. Because of autonegotiation, the actual status of a port can differ from how it was configured. To reconfigure a port, select a row, and click **Modify**.

To monitor or reconfigure a single port, right-click it, and then select **Port > Port Configuration** from the pop-up menu. The Port Configuration window (Figure 3-14) displays the status and settings of the port. Use the drop-down lists to reconfigure the port, and click **OK**.

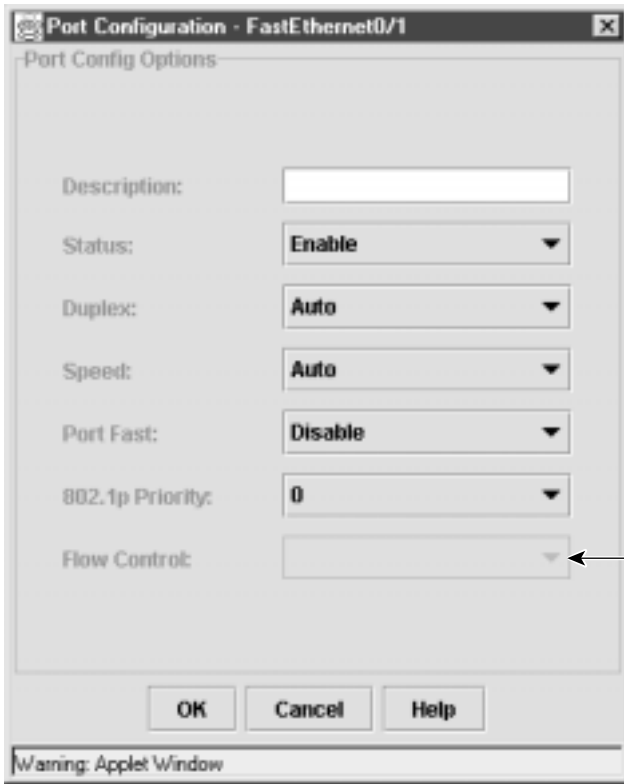
To make changes, select one or more rows in the table, and click **Modify**. The Group Port Configuration window (Figure 3-14) displays. When more than one port is selected, the window does not display the actual settings for the ports.

Figure 3-13 Port Configuration



Although you can configure settings for multiple mixed ports, some settings might not apply to all ports. For example, you can select half duplex from the drop-down list for a mixture of Ethernet and Gigabit Ethernet ports. The [“Guidelines for Configuring Ports”](#) section on page 3-41 describes some of the differences that apply to certain technologies.

You can also configure multiple ports on different switches. Select the ports by holding down the **Ctrl** key and left-clicking the ports. Right-click to display the pop-up menu, and select **Port > Port Configuration**. The Group Port Configuration pop-up (Figure 3-14) displays. You can use this window to change the ports settings for the selected ports, but the window does not display the actual port settings or VLAN information.

**Figure 3-14 Group Port Configuration Pop-up**

Parameters that do not apply to a port are grayed out.

45236



To enter a description for a port, select a row, and click **Describe**. The Basic Port Description window (Figure 3-15) appears. Enter a description, and click **OK**. To enter a description for more than one port, select the rows, and click **Describe**. Enter a description in the Advanced Port Description window (Figure 3-16), and click **OK**.

**Figure 3-15 Basic Port Description**

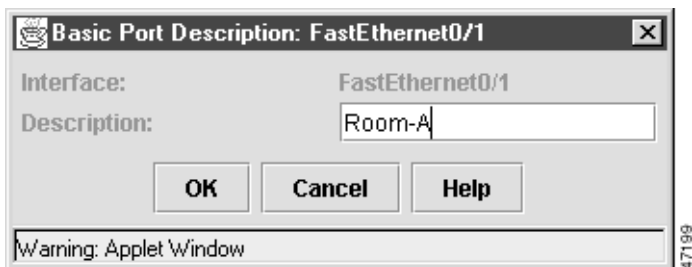
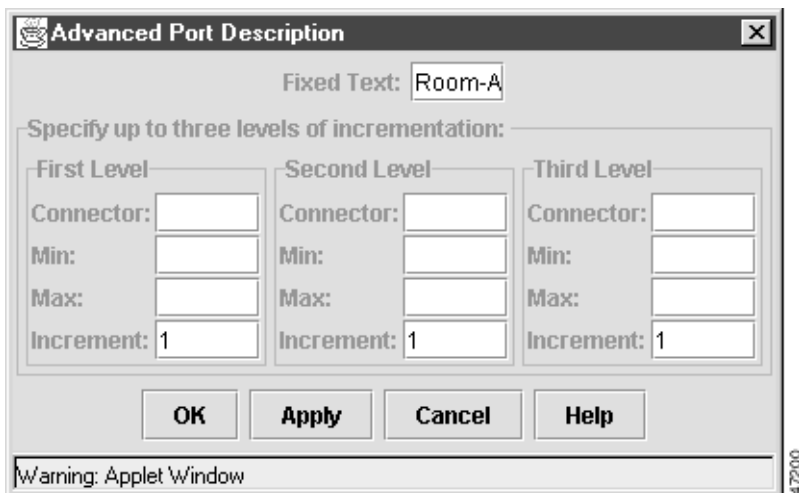


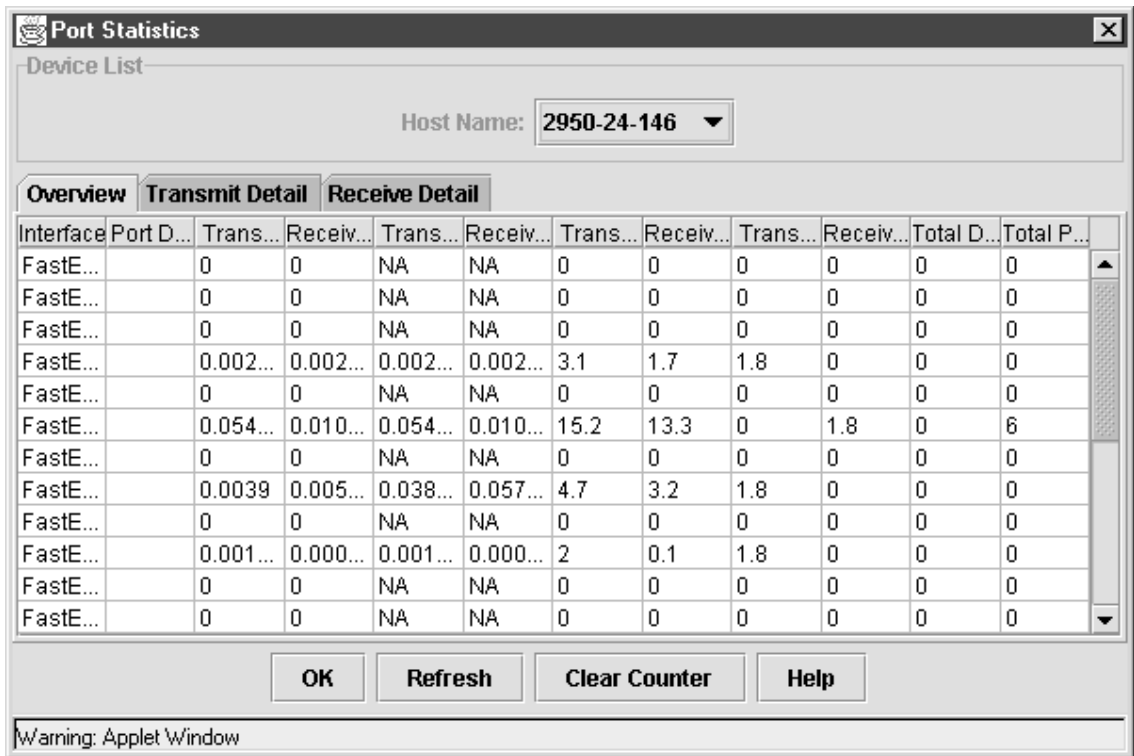
**Figure 3-16 Advanced Port Description**



## Port Statistics

To display detailed port statistics, click the switch, and select **Port > Port Statistics** from the Menu bar. The Port Statistics window (Figure 3-17) appears. The Port Statistics window displays detailed port statistics on link performance, dropped packages, total errors, etc.

**Figure 3-17 Port Statistics**



47213

## Port Search

To search for a port or a group of ports, click the switch, and select **Port > Port Search** from the Menu bar. The Port Search window ([Figure 3-18](#)) appears. Enter a description in the Find Port(s) with Description field, and click **Search**. The search results display all the ports that match the description.

 **Port Search** ✕

Find Ports With Description:

On These Devices:

Available Devices

Add ➡

⬅ Remove

Selected Devices

2950-24-146  
3512-140  
2950-24-145

Search

Search Results

| Device      | Interface | Description |
|-------------|-----------|-------------|
| <div></div> |           |             |

View Details ...

Done

Help

Warning: Applet Window

## CLI: Setting Speed and Duplex Parameters

Beginning in privileged EXEC mode, follow these steps to set the speed and duplex parameters on a port:

|        | Command                                   | Purpose                                                                                                                                                                                                                                                   |
|--------|-------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>                 | Enter global configuration mode.                                                                                                                                                                                                                          |
| Step 2 | <b>interface</b> <i>interface</i>         | Enter interface configuration mode, and enter the port to be configured.                                                                                                                                                                                  |
| Step 3 | <b>speed</b> {10   100   1000   auto}     | Enter the speed parameter for the port.                                                                                                                                                                                                                   |
| Step 4 | <b>duplex</b> {full   half   auto}        | Enter the duplex parameter for the port.<br><br><b>Note</b> The Gigabit Ethernet ports can operate in either half- or full-duplex mode when they are set to 10 or 100 Mbps, but when they are set to 1000 Mbps they can only operate in full-duplex mode. |
| Step 5 | <b>end</b>                                | Return to privileged EXEC mode.                                                                                                                                                                                                                           |
| Step 6 | <b>show running-config</b>                | Verify your entries.                                                                                                                                                                                                                                      |
| Step 7 | <b>copy running-config startup-config</b> | (Optional) Save your entry in the configuration file. This retains the configuration when the switch restarts.                                                                                                                                            |

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## CLI: Configuring Flow Control on Gigabit Ethernet Ports

The meaning of this parameter is described in [Table 3-1](#) on page 3-38.

Beginning in privileged EXEC mode, follow these steps to configure flow control on a Gigabit Ethernet port.

|        | Command                                     | Purpose                                                                                                        |
|--------|---------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>                   | Enter global configuration mode.                                                                               |
| Step 2 | <b>interface</b> <i>interface</i>           | Enter interface configuration mode, and enter the port to be configured.                                       |
| Step 3 | <b>flowcontrol</b> [asymmetric   symmetric] | Configure flow control for the port.                                                                           |
| Step 4 | <b>end</b>                                  | Return to privileged EXEC mode.                                                                                |
| Step 5 | <b>show running-config</b>                  | Verify your entries.                                                                                           |
| Step 6 | <b>copy running-config startup-config</b>   | (Optional) Save your entry in the configuration file. This retains the configuration when the switch restarts. |

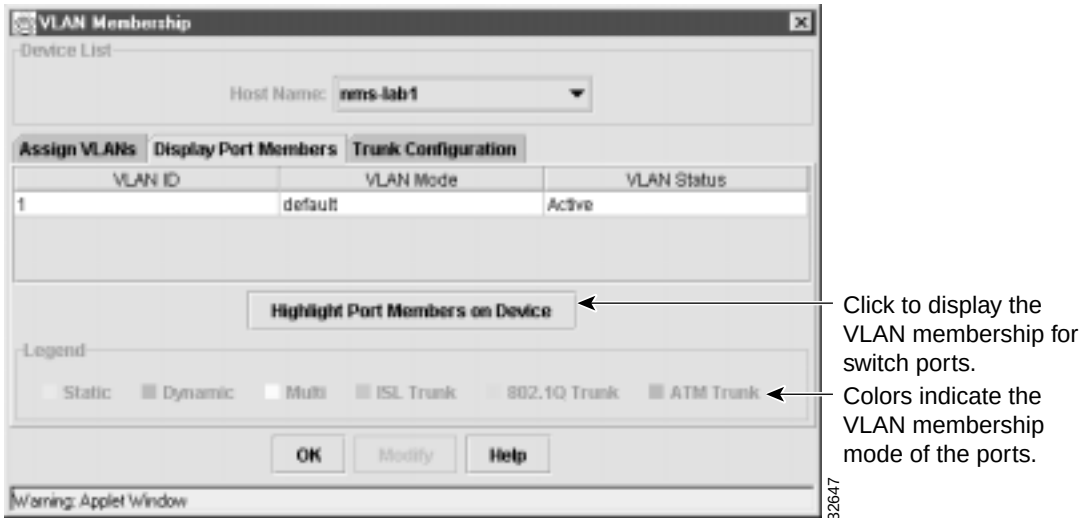
The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## Displaying VLAN Membership

The VLAN Membership window ([Figure 3-19](#)) displays the list of all the user-defined VLANs on the switch. By selecting a VLAN, you can display in Cluster Manager the ports that belong to that VLAN. You can also use this window to configure VLANs and trunks, as described in [Chapter 5, “Creating and Maintaining VLANs.”](#)

To display the VLANs that are active on a switch, right-click the switch chassis in Cluster Manager, and select **VLAN > VLAN Membership** from the menu bar.

To display the ports that belong to a given VLAN, select the **Display Port Members** tab. Select the VLAN ID, and click **Highlight Port Members on Device**. Cluster Manager highlights all the switch ports that belong to that VLAN. The legend on the page describes the meaning of each color.

**Figure 3-19 VLAN Membership**

## Upgrading or Reloading the Switch Software

You can upgrade cluster switches as a group or one at a time by using the Software Upgrade window (Figure 3-20) or the CLI. New software releases are posted on Cisco Connection Online (CCO) and are available through authorized resellers. Cisco also supplies a TFTP server that you can download from 48. Use the Software Upgrade window to upgrade several switches at once, or use the CLI to upgrade one switch at a time.

## Guidelines for Upgrading or Reloading Switch Software

You can upgrade all or some of the switches in a cluster at once, but the software first performs a series of checks.

## Configuring the Cisco TFTP Server to Upgrade Multiple Switches

The Cisco TFTP server application can handle multiple requests and sessions, but you must first disable the **TFTP Show File Transfer Progress** and the **Enable Logging** options to avoid TFTP server failures. If you are performing multiple-switch upgrades with a different TFTP server, it must be capable of managing multiple requests and sessions at the same time.

## CLI: Copying the Startup Configuration from the Switch to a PC or Server

When you make changes to a switch configuration, your changes become part of the running configuration. When you enter the command to save those changes to the startup configuration, the switch copies the configuration to the config.text file in Flash memory.

To ensure that you can recreate the configuration if a switch fails, you might want to copy the config.text file from the switch to a PC or server. The following procedure requires a configured TFTP server such as the Cisco TFTP server available on CCO.

Beginning in privileged EXEC mode, enter the following commands to copy a switch configuration file to the PC or server that has the TFTP server.

|        | Command                                                  | Purpose                                                                               |
|--------|----------------------------------------------------------|---------------------------------------------------------------------------------------|
| Step 1 | <b>copy flash:config.text tftp</b>                       | Copy the file in Flash memory to the root directory of the TFTP server.               |
| Step 2 | <b>Address or name of remote host?</b> <i>ip_address</i> | Follow the prompt for the IP address of the device where the TFTP server resides.     |
| Step 3 | <b>Destination filename [config.text]?</b> <i>yes/no</i> | Enter the name of the destination file. This could still be config.text.              |
| Step 4 |                                                          | Verify the copy by displaying the contents of the root directory on the PC or server. |

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.



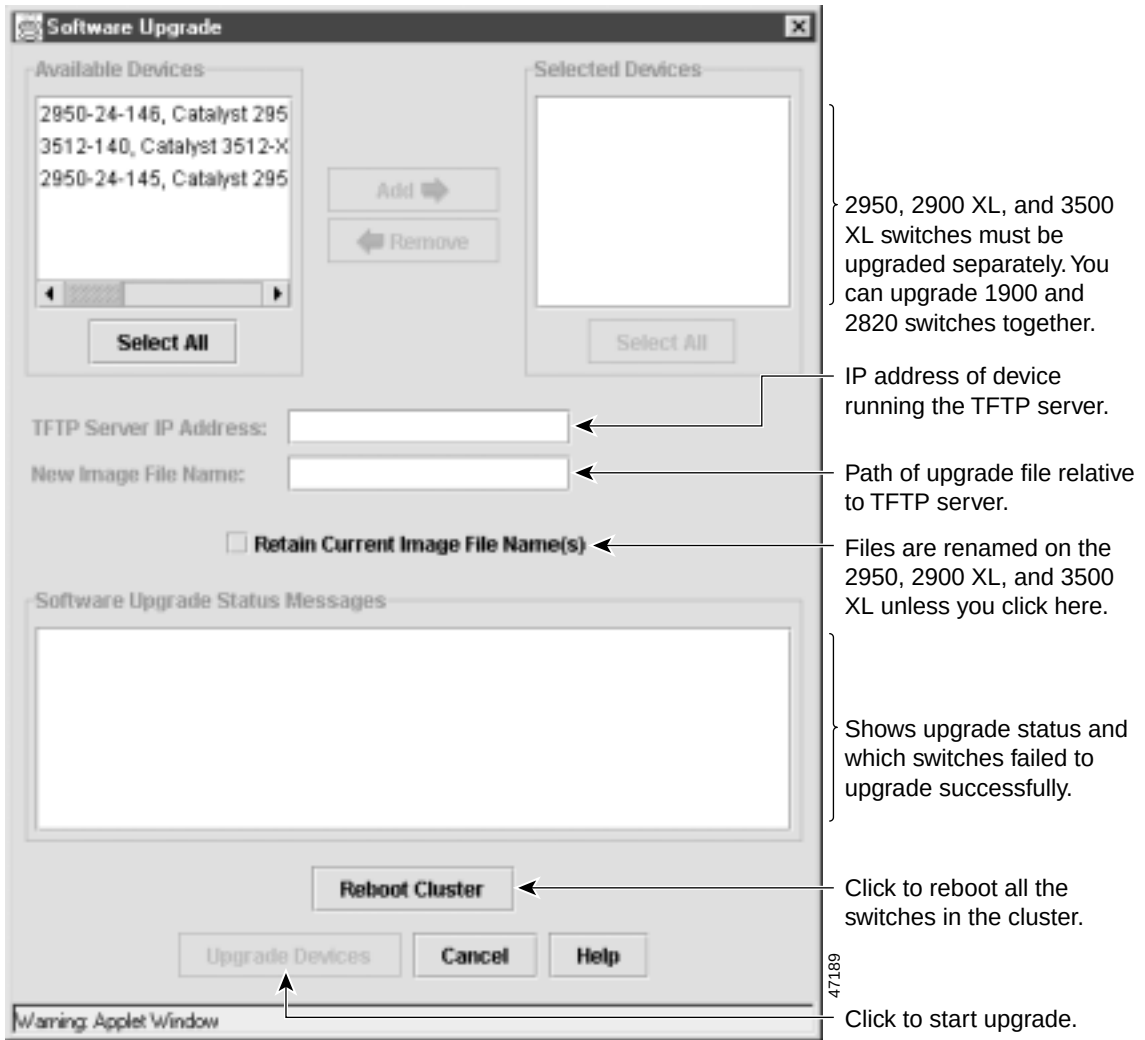
## Using the Software Upgrade Page to Upgrade Switch Software

In Cluster Manager, select **System > Software Upgrade** to display the Software Upgrade window ([Figure 3-20](#)). Enter the tar filename that contains the switch software image and the web-management code. You can enter just the filename or a path into the New Image File Name field. You do not need to enter a path if the image file is in directory you have defined as the TFTP root directory.

On Catalyst 2950 switches, new images are copied to Flash memory and do not affect the operation of the switch. The switch checks Flash memory to ensure that there is sufficient space before the upgrade takes place. If there is not enough space in Flash memory for the new and old images, the old image is deleted, and the new image is downloaded. If there is enough space, the new image is copied to the switch without replacing the old image, and after the new image is completely downloaded, the old one is erased. In this case, you can still reboot your switch using the old image if a failure occurs during the copy process.

New features provided by the software are not available until you reload the software.

Figure 3-20 Cluster Software Upgrade



## CLI: Upgrading a Standalone Switch

To upgrade a standalone switch, log into the switch by using Telnet, or connect to console port on the back of the switch.

The upgrade procedure consists of these steps:

- Changing the name of the *current* image file to the name of the *new* file you are copying and replacing the old image file with the new one by using the **tar** command.
- Disabling access to the HTML pages and deleting the existing HTML files before you upgrade the software to avoid a conflict with users accessing the web pages during the software upgrade.
- Reenabling access to the HTML pages after the upgrade is complete.

Beginning in privileged EXEC mode, follow these steps to upgrade the switch software:

|        | Command                                                                         | Purpose                                                                                                                                                                                  |
|--------|---------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>show version</b>                                                             | Verify that your switch has 16 MB of DRAM.<br><br>For example, check the line <code>cisco WS-C2950C (RC32300) processor with 1638K bytes of memory</code>                                |
| Step 2 | <b>show boot</b>                                                                | Display the name of the current (default) image file.                                                                                                                                    |
| Step 3 | <b>rename flash:</b> <i>current_image</i><br><b>flash:</b> <i>new_image.bin</i> | Rename the current image file to the name of the file that you downloaded, and replace the <i>tar</i> extension with <i>bin</i> . This step does not affect the operation of the switch. |
| Step 4 | <b>dir flash:</b>                                                               | Display the contents of Flash memory to verify the renaming of the file.                                                                                                                 |
| Step 5 | <b>configure terminal</b>                                                       | Enter global configuration mode.                                                                                                                                                         |
| Step 6 | <b>no IP http server</b>                                                        | Disable access to the switch HTML pages.                                                                                                                                                 |
| Step 7 | <b>end</b>                                                                      | Return to privileged EXEC mode.                                                                                                                                                          |

|         | Command                                                                   | Purpose                                                                                                                                                                                                                                                                          |
|---------|---------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 8  | <b>delete flash:html/*</b>                                                | Remove the HTML files.<br><br>Press <b>Enter</b> to confirm the deletion of each file. Do not press any other keys during this process.                                                                                                                                          |
| Step 9  | <b>delete flash:html/Snmp/*</b>                                           | For IOS release 11.2(8)SA5 and earlier running on 2900 XL switches, remove the files in the Snmp directory.<br><br>Make sure the S in <i>Snmp</i> is uppercase.<br><br>Press <b>Enter</b> to confirm the deletion of each file. Do not press any other keys during this process. |
| Step 10 | <b>tar /x<br/>tftp://server_ip_address//path/<br/>filename.tar flash:</b> | Use the <b>tar</b> command to copy the files into the switch Flash memory.<br><br>Depending on the TFTP server, you might need to enter only one slash (/) after the <i>server_ip_address</i> in the <b>tar</b> command.                                                         |
| Step 11 | <b>configure terminal</b>                                                 | Enter global configuration <b>mode</b> .                                                                                                                                                                                                                                         |
| Step 12 | <b>ip http server</b>                                                     | Reenable access to the switch HTTP pages.                                                                                                                                                                                                                                        |
| Step 13 | <b>end</b>                                                                | Return to privileged EXEC mode.                                                                                                                                                                                                                                                  |
| Step 14 | <b>reload</b>                                                             | Reload the new software.                                                                                                                                                                                                                                                         |

The “[Finding More Information About IOS Commands](#)” section on page 4-1 contains the path to the complete IOS documentation.

## CLI: Reloading or Upgrading Catalyst 2950, 2900 XL, or 3500 XL Member Switches

Because a member switch might not be assigned an IP address, command-line software upgrades through TFTP are managed through the command switch. Follow these steps to reload or upgrade the software on a Catalyst 2950, 2900 XL, or 3500 XL member switch:

- Step 1** In privileged EXEC mode on the command switch, display information about the cluster members:

```
switch# show cluster members
```

From the display, get the number of the member switch that needs to be upgraded. The member number is listed in the SN column of the display. You need the member number for Step 2.

- Step 2** Log into the member switch (for example, member number 1):

```
switch# rcommand 1
```

- Step 3** Start the TFTP copy as if you were initiating it from the command switch.

```
switch-1# tar /x tftp://server_ip_address//path/filename.tar flash:
Source IP address or hostname [server_ip_address]?
Source filename [path/filename]?
Destination filename [flash:new_image]?
Loading /path/filename.bin from server_ip_address (via!)
[OK - 843975 bytes]
```

- Step 4** Reload the new software with the following command:

```
switch-1# reload
System configuration has been modified. Save? [yes/no]:y
Proceed with reload? [confirm]
```

Press **Enter** to start the download.

You lose contact with the switch while it reloads the software. For more information on the **rcommand**, see the [“Understanding the CLI” section on page 2-25](#).

## CLI: Upgrading Catalyst 1900 or 2820 Member Switches

Because a member switch might not be assigned an IP address, command-line software upgrades through TFTP are managed through the command switch. Follow these steps to upgrade the software on a Catalyst 1900 or 2820 member switch:

- 
- Step 1** In privileged EXEC mode on the command switch, display information about the cluster members:

```
switch# show cluster members
```

From the display, get the number of the member switch that needs to be upgraded. The member number is listed in the SN column of the display. You need the member number for Step 2.

- Step 2** Log into the member switch (for example, member number 1):

```
switch# rcommand 1
```

- Step 3** For switches running standard edition software, enter the password (if prompted), access the Firmware Configuration menu from the menu console, and perform the upgrade.

The Telnet session accesses the menu console (the menu-driven interface) if the command switch is at privilege level 15. If the command switch is at privilege level 1, you are prompted for the password before accessing the menu console.

Follow the instructions in the installation and configuration guide that shipped with your switch. When the download is complete, the switch resets and begins using the new software.

- Step 4** For switches running Enterprise Edition Software, start the TFTP copy as if you were initiating it from the member switch:

```
switch-1# copy tftp://host/src_file opcode
```

For example, **copy tftp://spaniel/op.bin opcode** downloads new system operational code *op.bin* from the host *spaniel*.

You should see the TFTP successfully downloaded operational code message. When the download is complete, the switch resets and begins using the new software.

---

You can also perform the upgrade through the menu console Firmware Configuration menu. For more information, refer to the switch installation and configuration guide.

You lose contact with the switch while it reloads the software. For more information on the **rcommand**, see the [“Understanding the CLI” section on page 2-25](#).

## Reloading Switch Software

When you upgrade a switch, the switch continues to operate normally while the new software is copied to Flash memory. If Flash memory does not have enough space for two images, the new image is copied over the existing one. If Flash memory has enough space, the new image is copied to the selected switch but does not replace the current running image. Only after the new image is completely downloaded is the old one erased. If you experience a failure during the copy process, you can still reboot your switch by using the old image. The new software is loaded the next time you reboot.

If you group switches into a cluster, you can upgrade the entire cluster from Cluster Manager. For more information, see the [“Upgrading or Reloading the Switch Software” section on page 3-51](#).

## Configuring SNMP for a Cluster

The command switch manages SNMP communication for all switches in the cluster. The command switch forwards the set and get requests from SNMP applications to member switches, and it forwards the traps and other responses coming from the member switches to the appropriate management station. SNMP must be enabled for the Cluster Management features to work properly.



### Note

This section describes how the clustering software interacts with SNMP when a cluster is created. For more information on configuring SNMP, see the [“Configuring SNMP” section on page 4-41](#).

## Enabling or Disabling the SNMP Agent

You can enable or disable the SNMP agent on your cluster switches. By default, the SNMP agent is enabled on the Catalyst 1900, 2820, Catalyst 2950, 2900 XL, and 3500 XL switches. You cannot disable the agent on Catalyst 1900 and 2820 switches.

**Note**

---

SNMP must be enabled for the CMS graphing features.

---

## Configuring Community Strings for Cluster Switches

Use the SNMP Manager window ([Figure 3-21](#) and [Figure 3-22](#)) to enter read-write and read-only community strings on individual cluster switches. Community strings provide authentication in the exchange of SNMP messages.

Catalyst 2950, 2900 XL, and 3500 XL switches support an unlimited number of community strings of any length. When you configure a community string for these switches using SNMP Manager, do not use the @esN notation (N is the member-switch number) because this information is automatically appended to each string.

When a switch is removed from the cluster, community strings ending in @esN are removed. If the switch rejoins a cluster at a later time, the first read-only and read-write community strings from the command switch are appended with an @esN and propagated to the member switch.

The Catalyst 1900 and 2820 switches support up to four read-only and four read-write community strings that are 32 characters in length. Because a read-only and read-write community string from the command switch was propagated to the switch when it joined the cluster, you can configure up to three additional read-only and three read-write community strings. When you configure community strings for these switches through the SNMP Manager window, limit the string length to 27 characters because the @esN, where N can be up to two digits, is automatically appended to each string. Do not use the @esN notation in any community string you configure. If you enter a string longer than 27 characters, it is truncated to 27.

When removing community strings from cluster members, make sure not to remove the community strings propagated from the command switch when the switch joined the cluster. If you remove the propagated community string, the command switch cannot route SNMP packets to the member switch.



On Catalyst 2950, 2900 XL, and 3500 XL switches, the first read-only and read-write community string listed in the SNMP Manager window is propagated from the command switch. On Catalyst 1900 and 2820 switches, the last read-only and last read-write community string listed in the SNMP Manager window is propagated from the command switch.

**Figure 3-21 SNMP Manager for Catalyst 2950 Switches**

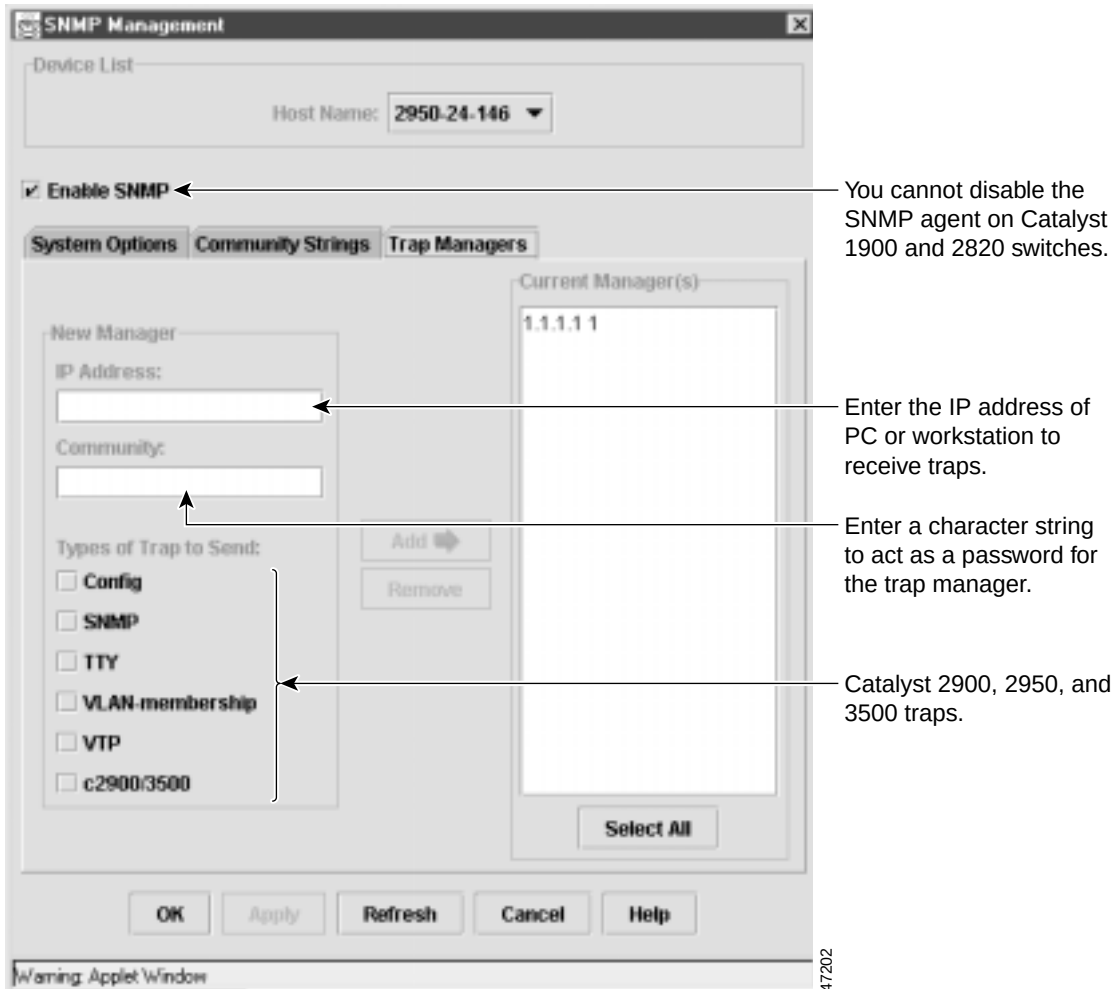
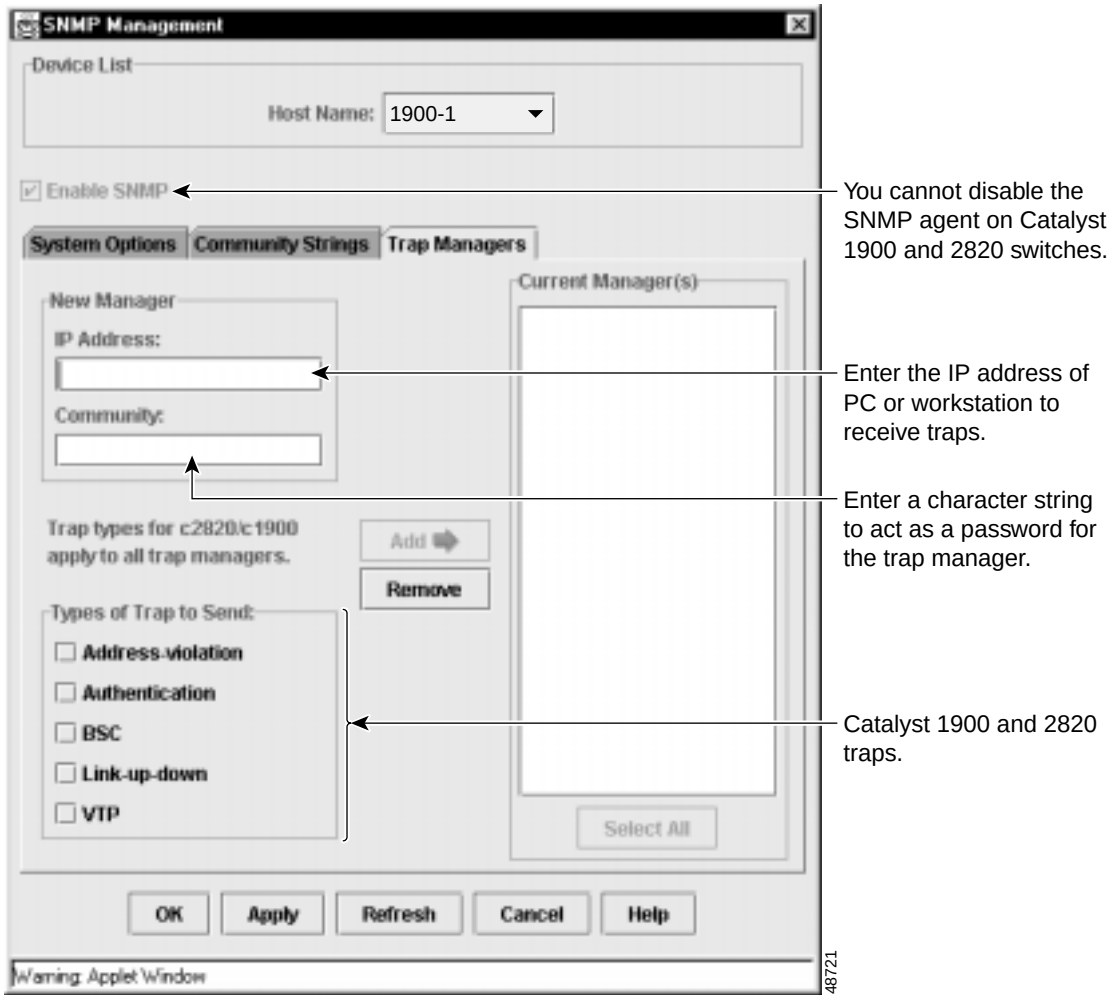


Figure 3-22 SNMP Manager for Catalyst 1900 and 2820 Switches



## Configuring Trap Managers and Enabling Traps

A trap manager is a management station that receives and processes traps. Traps are system alerts that the switch generates when certain events occur. If the member switch does not have an IP address, communication between the SNMP management station and the switch is managed by the command switch.

The command switch does not propagate its trap manager addresses or trap community strings to cluster members. By default, no trap manager is defined, and no traps are issued.

Catalyst 2950, 2900 XL, and 3500 XL switches support an unlimited number of trap managers. Community strings can be any length. When you configure a community string for these switches, do not use the @esN notation because this information is automatically appended to each string by the command switch.

[Table 3-2](#) describes the Catalyst 2950, 2900 XL, and 3500 XL switch traps. You can enable any or all of these traps and configure a trap manager to receive them.

**Table 3-2 2950, 2900 XL, and 3500 XL Switch Traps**

| Trap Type       | Description                                                                                                                |
|-----------------|----------------------------------------------------------------------------------------------------------------------------|
| Config          | Generates a trap when the switch configuration changes.                                                                    |
| TTY             | Generates a trap when the switch starts a management console CLI session.                                                  |
| VTP             | Generates a trap for VLAN Trunk Protocol (VTP) changes.                                                                    |
| SNMP            | Generates the supported SNMP traps.                                                                                        |
| VLAN Membership | Generates a trap for each VLAN Membership Policy Server (VMPS).                                                            |
| C2900/C3500     | Generates the switch-specific traps. These traps are in the private enterprise-specific Management Information Base (MIB). |

Catalyst 1900 and 2820 switches support up to four trap managers. When you configure community strings for these switches, limit the string length to 32 characters. When configuring traps on Catalyst 1900 and 2820 switches, you cannot configure individual trap managers to receive specific traps.

[Table 3-3](#) describes the Catalyst 1900 and 2820 switch traps. You can enable any or all of these traps, but these traps are received by all configured trap managers.

**Table 3-3 Catalyst 1900 and 2820 Switch Traps**

| Trap Type         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Address-violation | Generates a trap when the address violation threshold is exceeded.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Authentication    | Generates a trap when an SNMP request is not accompanied by a valid community string.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| BSC               | Generates a trap when the broadcast threshold is exceeded.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Link-up-down      | <p>Generates a link-down trap when a port is suspended or disabled for any of these reasons:</p> <ul style="list-style-type: none"> <li>Secure address violation (address mismatch or duplication)</li> <li>Network connection error (loss of linkbeat or jabber error)</li> </ul> <p>User disabling the port</p> <p>Generates a link-up trap when a port is enabled for any of these reasons:</p> <ul style="list-style-type: none"> <li>Presence of linkbeat</li> <li>Management intervention</li> <li>Recovery from an address violation or any other error</li> <li>STP action</li> </ul> |
| VTP               | Generates a trap when VTP changes occur.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |



## Managing Switches

---

This chapter describes how to use the device-management features of the Cluster Management Suite (CMS). The features described in this chapter can all be implemented through Visual Switch Manager (VSM), the web-based interface for managing standalone switches, or through Cluster Manager. If you need information on how to group your switches into a cluster, see [Chapter 3, “Creating and Managing Clusters.”](#)

This chapter describes two ways to configure switches:

- By using CMS windows to monitor and configure switches and ports.  
How-to procedures for using the windows are in the online help.
- By using the Cisco IOS command-line interface (CLI).  
CLI procedures are included for many tasks in this chapter. There are some features that can only be implemented by using the CLI.

## Finding More Information About IOS Commands

This guide describes only the IOS commands that have been created or changed for the Catalyst 2950 switches. These commands are further described in the *Catalyst 2950 Desktop Switch Command Reference*.

For information on other IOS Release 12.0 commands, refer to the Cisco IOS Release 12.0 documentation set available on Cisco.com.

# Managing Configuration Conflicts

Certain combinations of port features create configuration conflicts (see [Table 4-1](#)). If you try to enable incompatible features, CMS issues a warning message, and you cannot make the change. Reload the page to refresh CMS.

In [Table 4-1](#), **No** means that the two referenced features are incompatible and should not both be enabled; **yes** means that both can be enabled at the same time and will not cause an incompatibility conflict.

**Table 4-1** *Conflicting Features*

|                           | Protected Port | Port Group | Port Security | SPAN Port | Connect to Cluster? |
|---------------------------|----------------|------------|---------------|-----------|---------------------|
| <b>Protected Port</b>     | —              | Yes        | Yes           | No        | Yes                 |
| <b>Port Group</b>         | Yes            | —          | No            | No        | Yes                 |
| <b>Port Security</b>      | Yes            | No         | —             | No        | Yes                 |
| <b>SPAN Port</b>          | No             | No         | No            | —         | Yes                 |
| <b>Connect to Cluster</b> | Yes            | Yes        | Yes           | Yes       | —                   |

## Features, Default Settings, and Descriptions

You can configure the software features of this release by using any of the available interfaces. [Table 4-2](#) lists the most important features, their defaults, and where they are described in this guide.

**Table 4-2** *Default Settings and Where To Change Them*

| Feature                                              | Default Setting | Location of Feature and Feature Description                                                                     | Equivalent IOS CLI Procedure                                      |
|------------------------------------------------------|-----------------|-----------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| <b>Network Management</b>                            |                 |                                                                                                                 |                                                                   |
| Creating clusters                                    | None            | Cluster Builder<br>“Creating Clusters” section on page 3-5                                                      | “CLI: Creating a Cluster” section on page 3-8                     |
| Removing cluster members                             | None            | Cluster Builder<br>“Adding and Removing Member Switches” section on page 3-12                                   | “CLI: Removing a Member from a Cluster” section on page 3-16      |
| Reloading or Upgrading cluster software              | Enabled         | Cluster Manager: System > Software Upgrade<br>“Upgrading or Reloading the Switch Software” section on page 3-51 | “Upgrading or Reloading the Switch Software” section on page 3-51 |
| Displaying graphs                                    | Enabled         | Cluster Manager and Cluster Builder<br>“Displaying Link Graphs” section on page 6-1                             | —                                                                 |
| Configuring SNMP community strings and trap managers | None            | Cluster Manager: System > SNMP Management<br>“Configuring SNMP” section on page 4-41                            | —                                                                 |
| Configuring a port                                   | None            | Cluster Manager<br>“Monitoring and Configuring Ports” section on page 3-38                                      | “Configuring Ports” section on page 3-42                          |

**Table 4-2** *Default Settings and Where To Change Them (continued)*

| Feature                                             | Default Setting     | Location of Feature and Feature Description                                                                                        | Equivalent IOS CLI Procedure                                                                                                               |
|-----------------------------------------------------|---------------------|------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Device Management</b>                            |                     |                                                                                                                                    |                                                                                                                                            |
| Switch IP address, subnet mask, and default gateway | 0.0.0.0             | Cluster Manager: System > IP Management<br><a href="#">“Configuring IP Information” section on page 4-26</a>                       | <a href="#">“CLI: Assigning IP Information to the Switch” section on page 4-28</a>                                                         |
| Dynamic Host Configuration Protocol (DHCP)          | DHCP client enabled | <a href="#">“DHCP-Based Autoconfiguration” section on page 4-29</a>                                                                | —                                                                                                                                          |
| Management VLAN                                     | VLAN 1              | Cluster Manager: Cluster > Management VLAN<br><a href="#">“Changing the Management VLAN” section on page 3-34</a>                  | <a href="#">“Changing the Management VLAN” section on page 3-34</a>                                                                        |
| Domain name                                         | None                | Cluster Manager: System > IP Management<br><a href="#">“Specifying a Domain Name and Configuring the DNS” section on page 4-39</a> | Documentation set for Cisco IOS Release 12.0 on Cisco.com                                                                                  |
| Cisco Discovery Protocol (CDP)                      | Enabled             | —                                                                                                                                  | Documentation set for Cisco IOS Release 12.0 on Cisco.com                                                                                  |
| CoS and WRR                                         | Disabled            | Cluster Manager: Device > CoS and WRR<br><a href="#">“CoS and WRR” section on page 5-39</a>                                        | <a href="#">“CLI: Configuring CoS Priority Queues” section on page 5-42</a><br><a href="#">“CLI: Configuring WRR” section on page 5-43</a> |
| Address Resolution Protocol (ARP)                   | Enabled             | Cluster Manager: System > ARP Table<br><a href="#">“Managing the ARP Table” section on page 4-47</a>                               | Documentation set for Cisco IOS Release 12.0 on Cisco.com                                                                                  |



**Table 4-2** *Default Settings and Where To Change Them (continued)*

| Feature                    | Default Setting               | Location of Feature and Feature Description                                                                                                                                                                                                                                       | Equivalent IOS CLI Procedure                                                                                                                                    |
|----------------------------|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| System Time Management     | None                          | Cluster Manager: Cluster > System Time Management<br><br><a href="#">“Setting the System Date and Time” section on page 4-22</a>                                                                                                                                                  | Documentation set for Cisco IOS Release 12.0 on Cisco.com                                                                                                       |
| Static address assignment  | None assigned                 | Cluster Manager: Security > Address Management<br><br><a href="#">“Adding and Removing Static Addresses” section on page 4-55</a>                                                                                                                                                 | <a href="#">“CLI: Adding Static Addresses” section on page 4-57</a>                                                                                             |
| Dynamic address management | Enabled                       | Cluster Manager: Security > Address Management<br><br><a href="#">“Managing the MAC Address Tables” section on page 4-49</a> and <a href="#">“Changing the Address Aging Time” section on page 4-50</a>                                                                           | <a href="#">“CLI: Configuring the Aging Time” section on page 4-51</a><br><a href="#">“CLI: Removing Dynamic Address Entries” section on page 4-52</a>          |
| VLAN membership            | Static-access ports in VLAN 1 | Cluster Manager: VLAN > VLAN Membership<br><br><a href="#">“Displaying VLAN Membership” section on page 3-50</a><br><br><a href="#">“Assigning Static-Access Ports to a VLAN” section on page 5-5</a><br><br><a href="#">“CLI: Configuring a Trunk Port” section on page 5-32</a> | <a href="#">“CLI: Assigning Static-Access Ports to a VLAN” section on page 5-28</a><br><br><a href="#">“CLI: Configuring a Trunk Port” section on page 5-32</a> |
| VTP Management             | VTP server mode               | Cluster Manager: VLAN > VTP Management<br><br><a href="#">“Configuring VTP” section on page 5-12</a>                                                                                                                                                                              | <a href="#">“CLI: Configuring VTP Server Mode” section on page 5-14</a>                                                                                         |

**Table 4-2** *Default Settings and Where To Change Them (continued)*

| Feature                                        | Default Setting | Location of Feature and Feature Description                                                                           | Equivalent IOS CLI Procedure                                                                                                                                                                                                                               |
|------------------------------------------------|-----------------|-----------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Performance</b>                             |                 |                                                                                                                       |                                                                                                                                                                                                                                                            |
| Autonegotiation of duplex mode and port speeds | Enabled         | Cluster Manager: Port > Port Configuration<br><a href="#">“Monitoring and Configuring Ports” section on page 3-38</a> | <a href="#">“CLI: Setting Speed and Duplex Parameters” section on page 3-49</a>                                                                                                                                                                            |
| Gigabit Ethernet flow control                  | Any             | Cluster Manager > Port Configuration<br><a href="#">Configuring Ports, page 3-42</a>                                  | <a href="#">CLI: Configuring Flow Control on Gigabit Ethernet Ports, page 3-49</a>                                                                                                                                                                         |
| <b>Flooding Control</b>                        |                 |                                                                                                                       |                                                                                                                                                                                                                                                            |
| Storm control                                  | Disabled        | Cluster Manager: Port > Flooding Control<br><a href="#">“Configuring Flooding Controls” section on page 4-18</a>      | <a href="#">“CLI: Enabling Storm Control” section on page 4-20</a>                                                                                                                                                                                         |
| IGMP Snooping                                  | Enabled         | Cluster Manager: Device > IGMP Snooping<br><a href="#">“IGMP Snooping” section on page 4-64</a>                       | <a href="#">“CLI: Enabling or Disabling IGMP Snooping” section on page 4-67</a><br><a href="#">“CLI: Enabling IGMP Immediate-Leave Processing” section on page 4-68</a><br><a href="#">“CLI: Configuring a Multicast Router Port” section on page 4-79</a> |

**Table 4-2 Default Settings and Where To Change Them (continued)**

| Feature                       | Default Setting | Location of Feature and Feature Description                                                                                       | Equivalent IOS CLI Procedure                                                                                                                                                                                                                                                                                                                              |
|-------------------------------|-----------------|-----------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Network Redundancy</b>     |                 |                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                           |
| Hot Standby Router Protocol   | Disabled        | <a href="#">“Building a Redundant Cluster”</a> section on page 3-17                                                               | <a href="#">“CLI: Creating a Standby Group”</a> section on page 3-22<br><a href="#">“CLI: Adding Member Switches to a Standby Group”</a> section on page 3-24<br><a href="#">“CLI: Removing a Switch from a Standby Group”</a> section on page 3-25                                                                                                       |
| Spanning Tree Protocol        | Enabled         | Cluster Manager: Device > Spanning Tree Protocol<br><a href="#">“Configuring the Spanning Tree Protocol”</a> section on page 4-80 | <a href="#">“CLI: Disabling STP”</a> section on page 4-84<br><a href="#">“CLI: Changing the Path Cost”</a> section on page 4-97<br><a href="#">“CLI: Changing the Port Priority”</a> section on page 4-98<br><a href="#">“CLI: Enabling STP Port Fast”</a> section on page 4-97<br><a href="#">“CLI: Configuring STP Root Guard”</a> section on page 4-98 |
| Unidirectional link detection | Disabled        | —                                                                                                                                 | <a href="#">“CLI: Configuring UniDirectional Link Detection”</a> section on page 4-100                                                                                                                                                                                                                                                                    |
| Port grouping                 | None assigned   | Cluster Manager: Port > Port Grouping (EC)<br><a href="#">“Creating EtherChannel Port Groups”</a> section on page 4-11            | <a href="#">“CLI: Creating EtherChannel Port Groups”</a> section on page 4-15                                                                                                                                                                                                                                                                             |

**Table 4-2** *Default Settings and Where To Change Them (continued)*

| Feature                           | Default Setting | Location of Feature and Feature Description                                                                                 | Equivalent IOS CLI Procedure                                                       |
|-----------------------------------|-----------------|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| <b>Diagnostics</b>                |                 |                                                                                                                             |                                                                                    |
| SPAN port monitoring              | Disabled        | Cluster Manager: Port > Switch Port Analyzer (SPAN)<br><a href="#">“Enabling Switch Port Analyzer” section on page 4-15</a> | <a href="#">“CLI: Enabling Switch Port Analyzer” section on page 4-17</a>          |
| Console, buffer, and file logging | Disabled        | —                                                                                                                           | Documentation set for Cisco IOS Release 12.0 on Cisco.com                          |
| Remote monitoring (RMON)          | Disabled        | <a href="#">“Configuring the Switch for Remote Monitoring” section on page 4-108</a>                                        | Documentation set for Cisco IOS Release 12.0 on Cisco.com                          |
| <b>Security</b>                   |                 |                                                                                                                             |                                                                                    |
| Password                          | None            | <a href="#">“Changing the Password” section on page 4-11</a>                                                                | <a href="#">“Recovering from a Lost or Forgotten Password” section on page 7-6</a> |
| Addressing security               | Disabled        | Cluster Manager: Security > Address Management<br><a href="#">“Adding Secure Addresses” section on page 4-52</a>            | <a href="#">“CLI: Adding Secure Addresses” section on page 4-54</a>                |
| Trap manager                      | 0.0.0.0         | Cluster Manager: System > SNMP Management<br><a href="#">“CLI: Adding a Trap Manager” section on page 4-47</a>              | <a href="#">“CLI: Adding a Trap Manager” section on page 4-47</a>                  |
| Community strings                 | public          | Cluster Manager: System > SNMP Configuration<br><a href="#">“Entering Community Strings” section on page 4-42</a>           | Documentation set for Cisco IOS Release 12.0 on Cisco.com                          |

**Table 4-2** Default Settings and Where To Change Them (continued)

| Feature        | Default Setting | Location of Feature and Feature Description                                                                | Equivalent IOS CLI Procedure                                                   |
|----------------|-----------------|------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| Port security  | Disabled        | Cluster Manager: Security > Port Security<br><a href="#">“Enabling Port Security” section on page 4-58</a> | <a href="#">“CLI: Enabling Port Security” section on page 4-61</a>             |
| TACACS+        | Disabled        | <a href="#">“Configuring TACACS+” section on page 4-101</a>                                                | <a href="#">“CLI Procedures for Configuring TACACS+” section on page 4-102</a> |
| Protected Port | Disabled        | <a href="#">“Configuring Protected Ports” section on page 4-100</a>                                        | <a href="#">“Configuring Protected Ports” section on page 4-100</a>            |

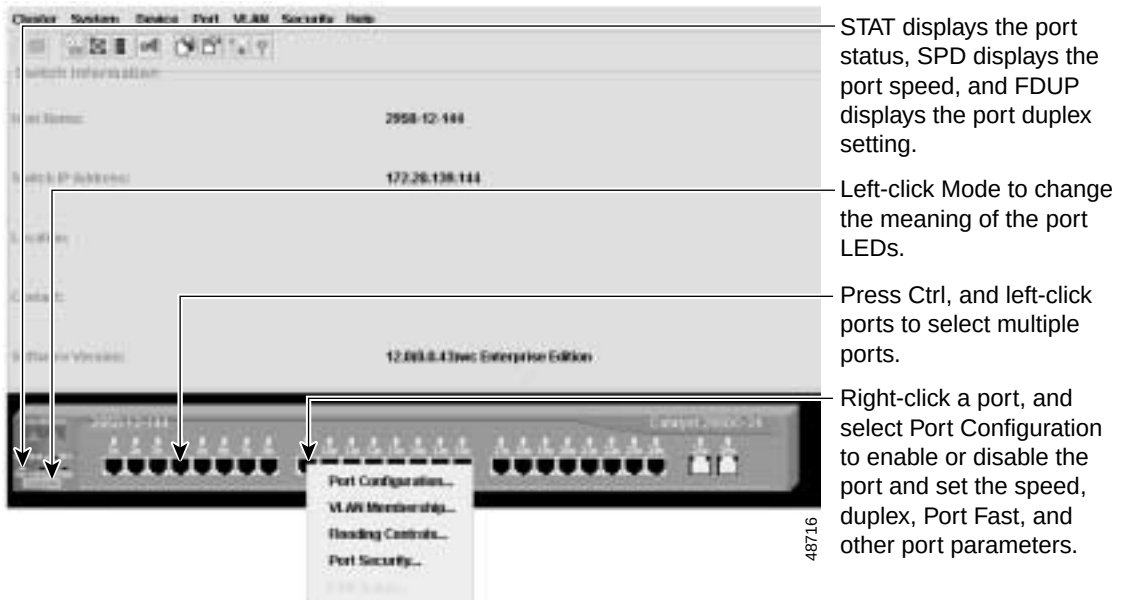
## Configuring Standalone Switches

Visual Switch Manager (VSM) is one of the CMS interfaces for managing individual switch features. If you are configuring a standalone switch, you can access VSM directly by entering the switch IP address in the browser **Location** field (Netscape Communicator) or **Address** field (Internet Explorer). Click **Cluster Management Suite or Visual Switch Manager** on the Cisco Systems Access Page, and the switch senses that the IP address refers to a standalone switch and displays the VSM home page.

**Note**

Menu options are arranged slightly differently in VSM than in Cluster Manager. For the complete list of the options available, see [“VSM Menu Bar Options” section on page 2-22](#).

A browser plug-in is required to access the HTML interface. For information on installing the plug-in, refer to the *Release Notes for the Catalyst 2950 Cisco IOS Release 12.0(5)WC(1)*.

**Figure 4-1 VSM Home Page**

## Enabling the Switch as a Command Switch

Before you can create a cluster, one switch must be assigned an IP address and enabled as the command switch. See the [“Command Switch Requirements”](#) section on page 3-3 to ensure that the switch meets all the requirements.

To enable a command switch, select **Cluster > Cluster Command Configuration** from the menu bar, and select **Enable** on the Cluster Configuration window. You can use up to 28 characters to name your cluster. After you have enabled the command switch, select **Cluster > Cluster Builder** to begin building your cluster. To build your cluster by using the CLI, see the [“CLI: Creating a Cluster”](#) section on page 3-8.

**Figure 4-2 Enable Command Switch**

## Changing the Password

If you change the enable secret password, your connection with the switch breaks, and the browser prompts you for the new password. You can only change a password by using the CLI. If you have forgotten your password, see the [“Recovering from a Lost or Forgotten Password”](#) section on page 7-6.

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## Creating EtherChannel Port Groups

Use the Port Group (EtherChannel) window (Figure 4-4) to create Fast EtherChannel and Gigabit EtherChannel port groups. These port groups act as single logical ports for high-bandwidth connections between switches or between switches and servers.

To display this window, select **Port > Port Grouping (EtherChannel)** from the menu bar.

For the restrictions that apply to port groups, see the [“Managing Configuration Conflicts”](#) section on page 4-2.

## Understanding EtherChannel Port Grouping

This software release supports two different types of port groups: source-based forwarding port groups and destination-based forwarding port groups.

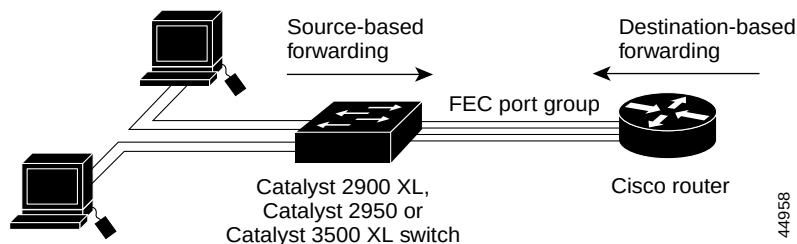
Source-based forwarding port groups distribute packets forwarded to the group based on the source address of incoming packets. You can configure up to eight ports in a source-based forwarding port group. Source-based forwarding is enabled by default.

Destination-based port groups distribute packets forwarded to the group based on the destination address of incoming packets. You can configure up to eight ports in a group.

You can create up to 6 port groups of all source-based, all destination-based, or a combination of source- and destination-based ports. All ports in the group must be of the same type; for example, they must be all source based or all destination based. You can independently configure port groups that link switches, but you must consistently configure both ends of a port group.

In [Figure 4-3](#), a port group of two workstations communicates with a router. Because the router is a single-MAC address device, source-based forwarding ensures that the switch uses all available bandwidth to the router. The router is configured for destination-based forwarding because the large number of stations ensures that the traffic is evenly distributed through the port-group ports on the router.

**Figure 4-3 Source-Based Forwarding**



The switch treats the port group as a single logical port; therefore, when you create a port group, the switch uses the configuration of the first port for all ports added to the group. If you add a port and change the forwarding method, it changes the forwarding for all ports in the group. After the group is created,



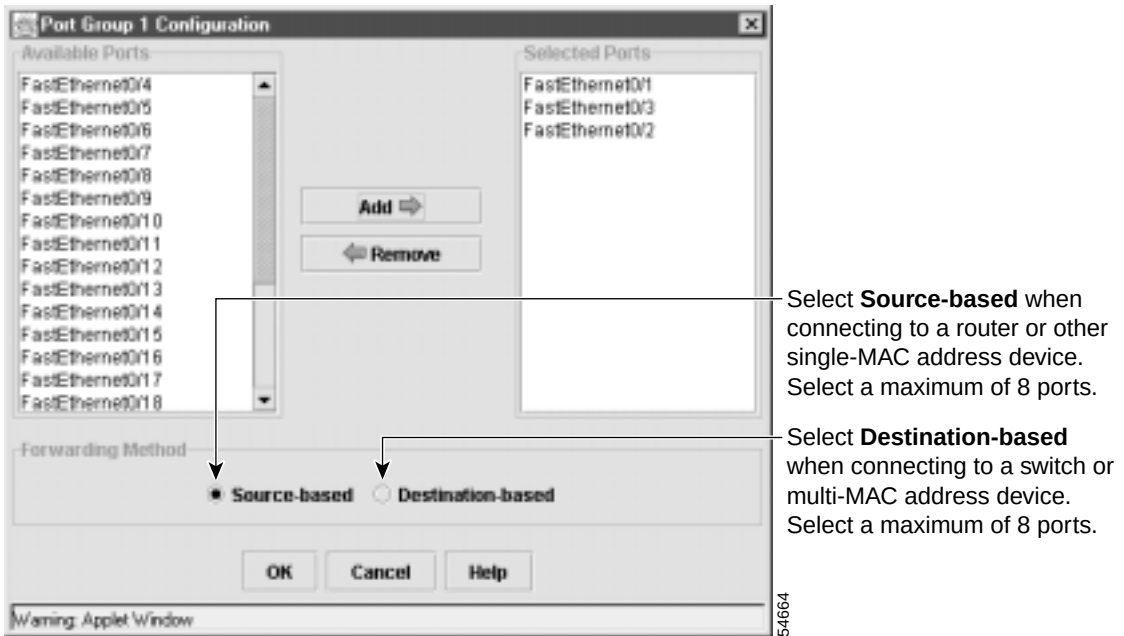
changing STP or VLAN membership parameters for one port in the group automatically changes the parameters for all ports. Each port group has one port that carries all unknown multicast, broadcast, and STP packets.

**Figure 4-4 Port Grouping (EtherChannel)**

| Group Number | Members | Forwarding Method |
|--------------|---------|-------------------|
| 1            |         |                   |
| 2            |         |                   |
| 3            |         |                   |
| 4            |         |                   |
| 5            |         |                   |
| 6            |         |                   |

Warning: Applet Window

Figure 4-5 Port Group Configuration



## Port Group Restrictions on Static-Address Forwarding

The following restrictions apply to entering static addresses that are forwarded to port groups:

- If the port group forwards based on the source MAC address (the default), configure the static address to forward to all ports in the group. This method eliminates the chance of lost packets.
- If the port group forwards based on the destination address, configure the static address to forward to only one port in the port group. This method avoids the possible transmission of duplicate packets. For more information, see [“Adding and Removing Static Addresses” section on page 4-55](#).

## CLI: Creating EtherChannel Port Groups

Beginning in privileged EXEC mode, follow these steps to create a two-port group:

|        | Command                                      | Purpose                                                                                            |
|--------|----------------------------------------------|----------------------------------------------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>                    | Enter global configuration mode.                                                                   |
| Step 2 | <b>interface</b> <i>interface</i>            | Enter interface configuration mode, and enter the port of the first port to be added to the group. |
| Step 3 | <b>port group 1 distribution destination</b> | Assign the port to group 1 with destination-based forwarding.                                      |
| Step 4 | <b>interface</b> <i>interface</i>            | Enter the second port to be added to the group.                                                    |
| Step 5 | <b>port group 1 distribution destination</b> | Assign the port to group 1 with destination-based forwarding.                                      |
| Step 6 | <b>end</b>                                   | Return to privileged EXEC mode.                                                                    |
| Step 7 | <b>show running-config</b>                   | Verify your entries.                                                                               |

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## Enabling Switch Port Analyzer

You can monitor traffic on a given port by forwarding incoming and outgoing traffic on the port to another port in the same VLAN. Use the Switch Port Analyzer (SPAN) window ([Figure 4-6](#)) to enable port monitoring on a port, and use the Modify the Ports Being Monitored window ([Figure 4-7](#)) to select the port to be monitored. A SPAN port cannot monitor ports in a different VLAN, and a SPAN port must be a static-access port. You can have only one assigned monitor port at any given time. If you select another port as the monitor port, the previous monitor port is disabled, and the newly selected port becomes the monitor port.

To display this window, select **Port > Switch Port Analyzer** from the menu bar. For the restrictions that apply to SPAN ports, see the [“Managing Configuration Conflicts”](#) section on page 4-2.

**Figure 4-6 Switch Port Analyzer (SPAN)**

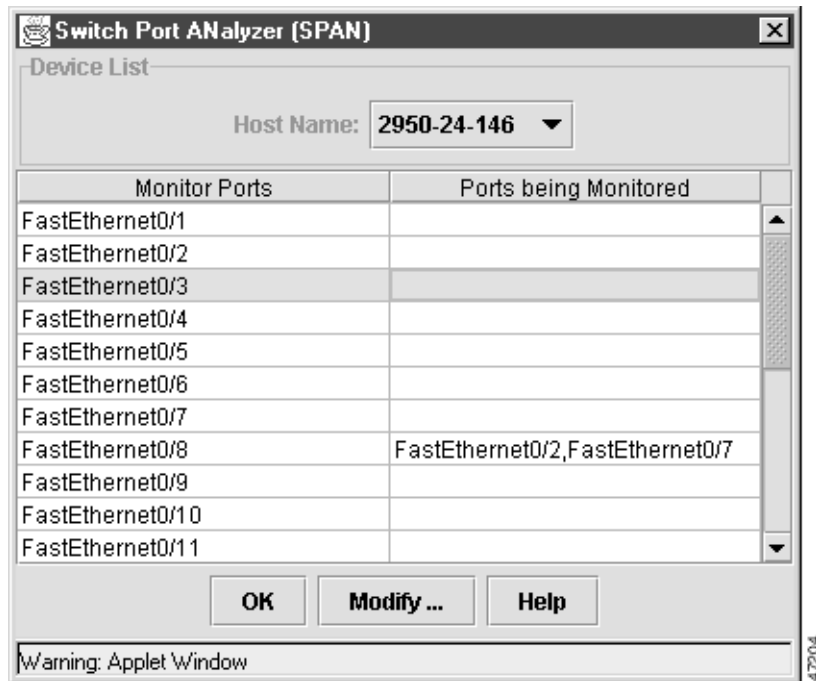
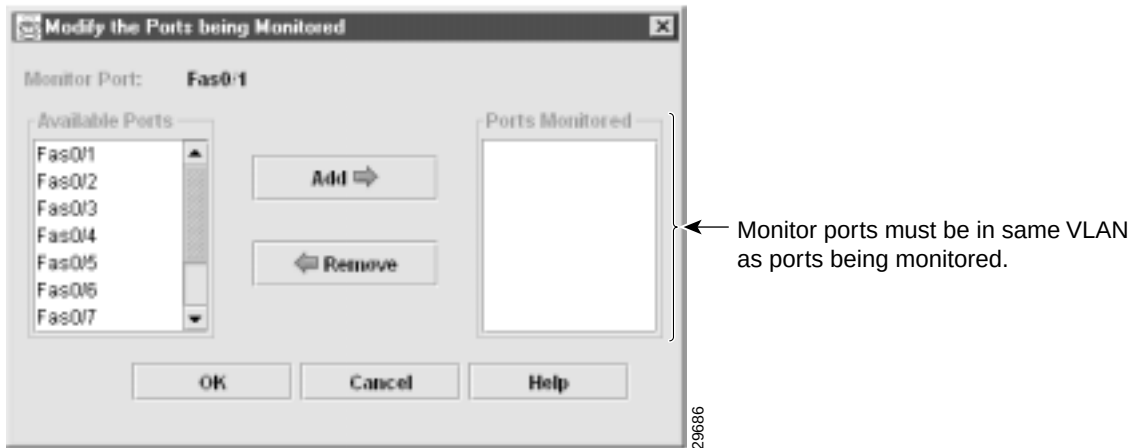


Figure 4-7 Modify the Ports Being Monitored



## CLI: Enabling Switch Port Analyzer

Beginning in privileged EXEC mode, follow these steps to enable switch port analyzer:

|        | Command                              | Purpose                                                                               |
|--------|--------------------------------------|---------------------------------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>            | Enter global configuration mode.                                                      |
| Step 2 | <b>interface</b> <i>interface</i>    | Enter interface configuration mode, and enter the port that acts as the monitor port. |
| Step 3 | <b>port monitor</b> <i>interface</i> | Enable port monitoring on the port.                                                   |
| Step 4 | <b>end</b>                           | Return to privileged EXEC mode.                                                       |
| Step 5 | <b>show running-config</b>           | Verify your entries.                                                                  |

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## CLI: Disabling Switch Port Analyzer

Beginning in privileged EXEC mode, follow these steps to disable switch port analyzer:

|        | Command                                 | Purpose                                                                            |
|--------|-----------------------------------------|------------------------------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>               | Enter global configuration mode.                                                   |
| Step 2 | <b>interface</b> <i>interface</i>       | Enter interface configuration mode, and enter the port number of the monitor port. |
| Step 3 | <b>no port monitor</b> <i>interface</i> | Disable port monitoring on the port.                                               |
| Step 4 | <b>end</b>                              | Return to privileged EXEC mode.                                                    |
| Step 5 | <b>show running-config</b>              | Verify your entries.                                                               |

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## Configuring Flooding Controls

Use the Flooding Controls window ([Figure 4-8](#)) to block the forwarding of unnecessary flooded traffic.

To display this window, select **Port > Flooding Controls** from the menu bar.

## Enabling Storm Control

A packet storm occurs when a large number of broadcast, unicast, or multicast packets are received on a port. Forwarding these packets can cause the network to slow down or to time out. Storm control is configured for the switch as a whole but operates on a per-port basis. By default, storm control is disabled.

Storm control uses high and low thresholds to block and then restore the forwarding of broadcast, unicast, or multicast packets. You can also set the switch to shut down the port when the rising threshold is reached.

The rising threshold is the number of packets that a switch port can receive before forwarding is blocked. The falling threshold is the number of packets below which the switch resumes normal forwarding. In general, the higher the threshold, the less effective the protection against broadcast storms. The maximum half-duplex transmission on a 100BaseT link is 148,000 packets per second, but you can enter a threshold of up to 4294967295 broadcast packets per second.

To configure storm control, right-click a switch chassis in Cluster Manager, and select **Port > Flooding Controls**. Select one of the Storm tabs (Figure 4-8), select a port, and click **Modify**. Set the parameters on the Flooding Controls Configuration pop-up (Figure 4-9).

**Figure 4-8 Flooding Controls**

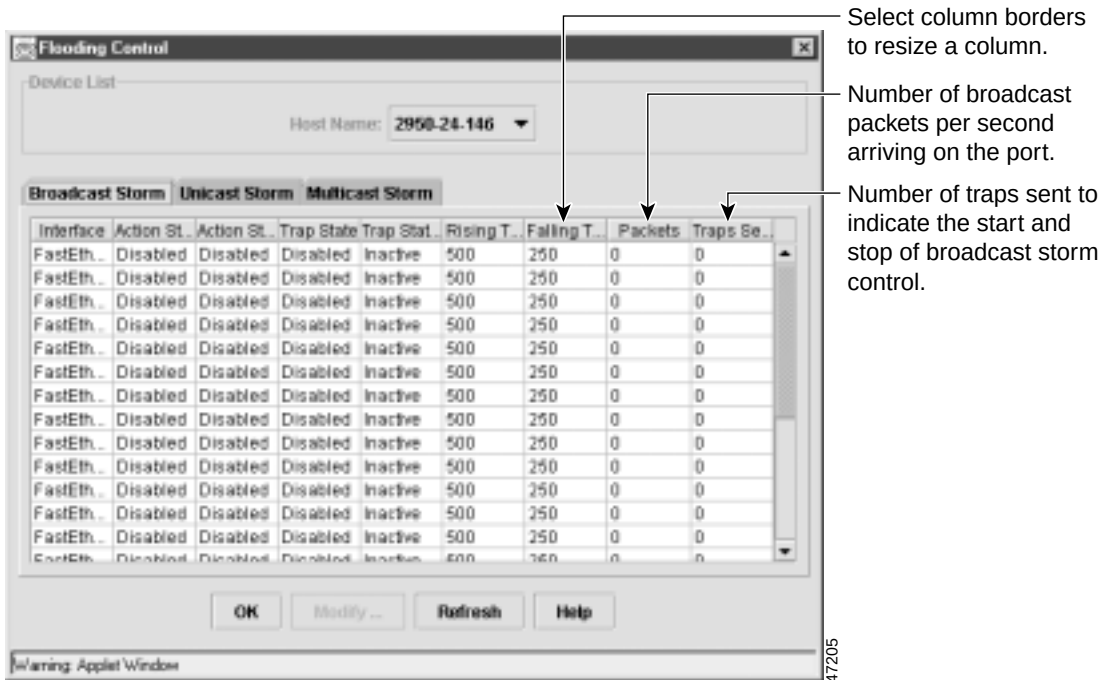
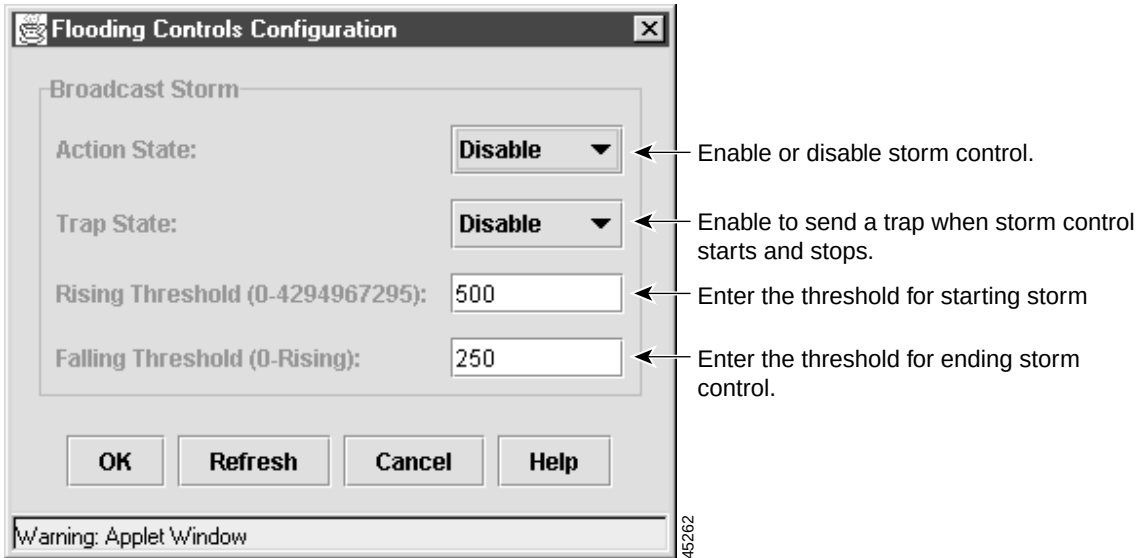


Figure 4-9 Flooding Controls Configuration Pop-up



## CLI: Enabling Storm Control

With the exception of the **broadcast** keyword, the following procedure could also be used to enable storm control for unicast or multicast packets.

Beginning in privileged EXEC mode, follow these steps to enable broadcast-storm control.

|        | Command                                                                                                                                 | Purpose                                                                                                                                     |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>                                                                                                               | Enter global configuration mode.                                                                                                            |
| Step 2 | <b>interface</b> <i>interface</i>                                                                                                       | Enter interface configuration mode, and enter the port to configure.                                                                        |
| Step 3 | <b>port storm-control broadcast</b><br><b>[threshold {rising</b> <i>rising-number</i><br><b>falling</b> <i>falling-number</i> <b>}]</b> | Enter the rising and falling thresholds for broadcast packets.<br><br>Make sure the rising threshold is greater than the falling threshold. |



|        | Command                                              | Purpose                                                                                     |
|--------|------------------------------------------------------|---------------------------------------------------------------------------------------------|
| Step 4 | <b>port storm-control trap</b>                       | Generate an SNMP trap when the traffic on the port crosses the rising or falling threshold. |
| Step 5 | <b>end</b>                                           | Return to privileged EXEC mode.                                                             |
| Step 6 | <b>show port storm-control</b><br><i>[interface]</i> | Verify your entries.                                                                        |

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## CLI: Disabling Storm Control

Beginning in privileged EXEC mode, follow these steps to disable broadcast-storm control.

|        | Command                                              | Purpose                                                              |
|--------|------------------------------------------------------|----------------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>                            | Enter global configuration mode.                                     |
| Step 2 | <b>interface</b> <i>interface</i>                    | Enter interface configuration mode, and enter the port to configure. |
| Step 3 | <b>no port storm-control broadcast</b>               | Disable port storm control.                                          |
| Step 4 | <b>end</b>                                           | Return to privileged EXEC mode.                                      |
| Step 5 | <b>show port storm-control</b><br><i>[interface]</i> | Verify your entries.                                                 |

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

# Managing the System Date and Time

Use the System Time Management window (Figure 4-10) to set the system time for a switch or enable an external source such as Network Time Protocol (NTP) to supply time to the switch.

You can use this window to set the switch time by using one of the following techniques:

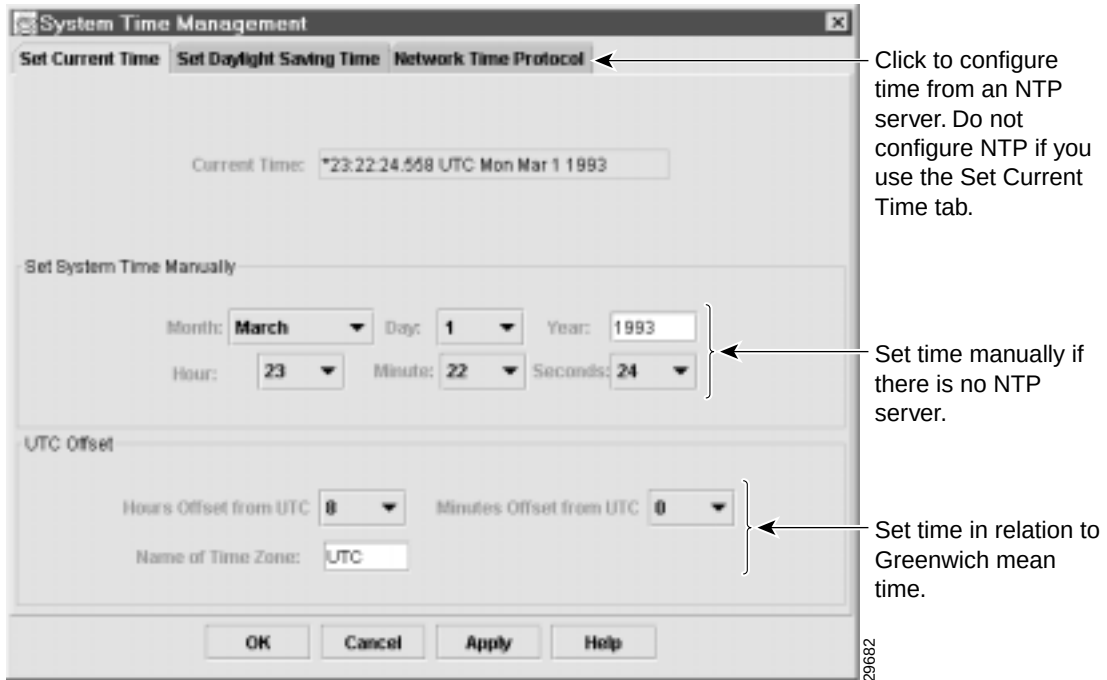
- Manually setting the system time (including daylight saving time) and date
- Configuring the switch to run in NTP client mode and to receive time information from an NTP server
- Configuring the switch to run in NTP broadcast-client mode and to receive information from an NTP broadcast server

To display this window, select **Cluster > System Time Management** from the menu bar.

## Setting the System Date and Time

Enter the date and a 24-hour clock time setting on the System Time Management window. If you are entering the time for an American time zone, enter the three-letter abbreviation for the time zone in the **Name of Time Zone** field, such as PST for Pacific standard time. If you are identifying the time zone by referring to Greenwich mean time, enter UTC (universal coordinated time) in the **Name of Time Zone** field. You then must enter a negative or positive number as an offset to indicate the number of time zones between the switch and Greenwich, England. Enter a negative number if the switch is west of Greenwich, England, and east of the international date line. For example, California is eight time zones west of Greenwich, so you would enter -8 in the **Hours Offset From UTC** field. Enter a positive number if the switch is east of Greenwich. You can also enter negative and positive numbers for minutes.

You can also set the date and time by using the CLI. “[Finding More Information About IOS Commands](#)” section on page 4-1 contains the path to the complete IOS documentation.

**Figure 4-10 System Time Management**

## Configuring Daylight Saving Time

To configure daylight saving time, click the **Set Daylight Saving Time** tab (Figure 4-11). You can configure the switch to change to daylight saving time on a particular day every year, on a day that you enter, or not at all.

**Figure 4-11 Set Daylight Savings Time Tab**

32641

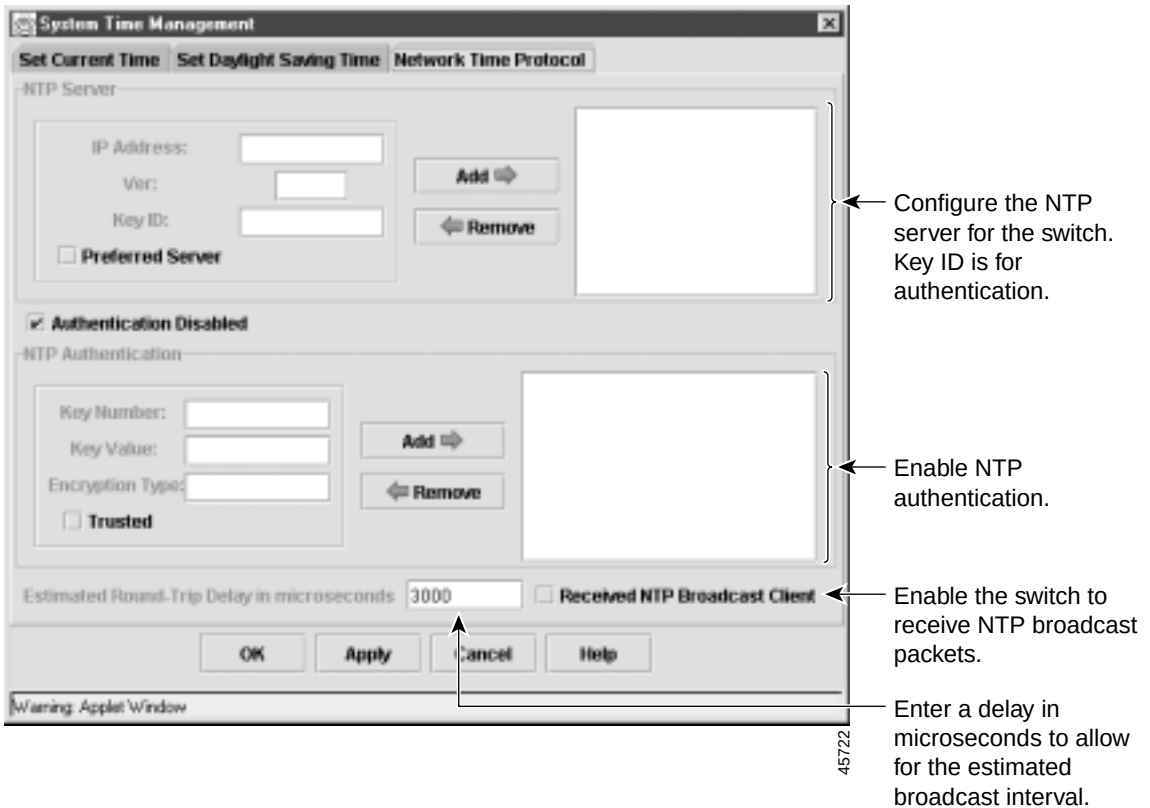
## Configuring the Network Time Protocol

In complex networks, it is often prudent to distribute time information from a central server. The NTP can distribute time information by responding to requests from clients or by broadcasting time information. You can use the Network Time Protocol window (Figure 4-12) to enable these options and to enter authentication information to accompany NTP client requests.

To display this window, click **Network Time Protocol** on the System Time Management window.

You can also configure NTP by using the CLI. [“Finding More Information About IOS Commands” section on page 4-1](#) contains the path to the complete IOS documentation.

Figure 4-12 Network Time Protocol



## Configuring the Switch as an NTP Client

You configure the switch as an NTP client by entering the IP addresses of up to ten NTP servers in the IP Address field. Click **Preferred Server** to specify which server should be used first. You can also enter an authentication key to be used as a password when requests for time information are sent to the server.

## Enabling NTP Authentication

To ensure the validity of information received from NTP servers, you can authenticate NTP messages with public-key encryption. This procedure must be coordinated with the administrator of the NTP servers: the information you enter on this window will be matched by the servers to authenticate it.

Click **Help** for more information about entering information in the Key Number, Key Value, and Encryption Type fields.

## Configuring the Switch for NTP Broadcast-Client Mode

You can configure the switch to receive NTP broadcast messages if there is an NTP broadcast server, such as a router, broadcasting time information on the network. You can also enter a delay in the Estimated Round-Trip Delay field to account for round-trip delay between the client and the NTP broadcast server.

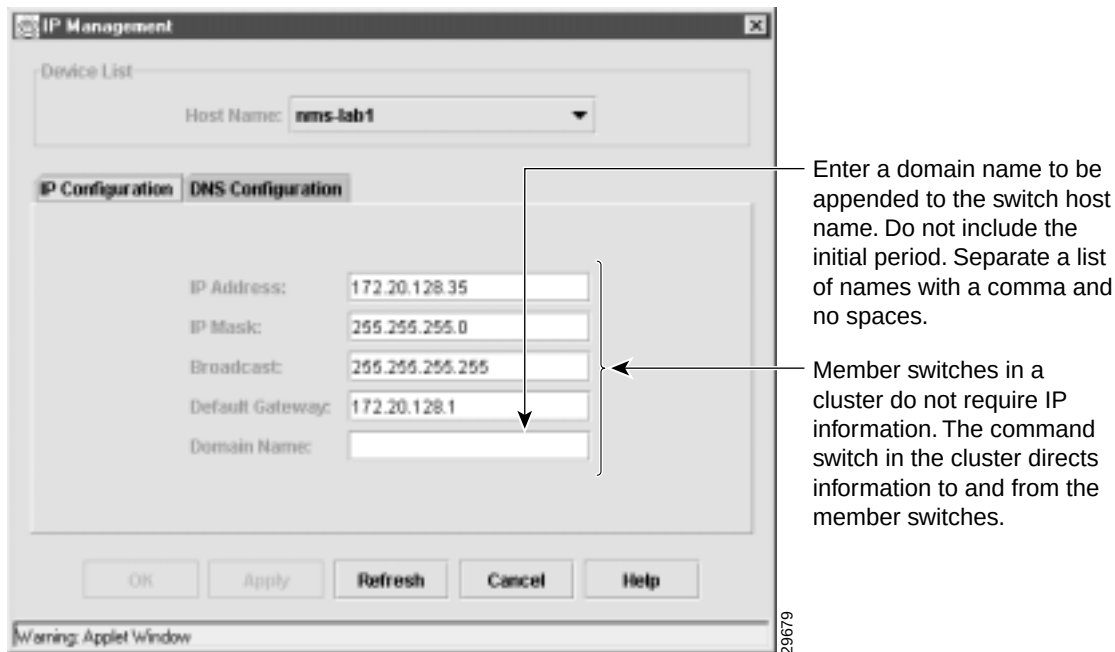
# Configuring IP Information

Use the IP Management window ([Figure 4-13](#)) to change or enter IP information for the switch. Some of this information, such as the IP address was previously entered.

You can use this window to perform the following tasks:

- Assign IP information.
- Remove an IP address.
- Specify a domain name, and configure the Domain Name System (DNS) server.

To display this window, select **System > IP Management** from the menu bar.

**Figure 4-13 IP Management—IP Configuration Tab**

You can assign IP information to your switch in these ways:

- Using the Setup program (refer to the *Release Notes for the Catalyst 2950 Cisco IOS Release 12.0(5)WC(1)*)
- Manually assigning an IP address
- Using DHCP-based autoconfiguration

## Manually Assigning IP Information to the Switch

You can manually assign an IP address, mask, and default gateway to the switch through the management console. This information is displayed in the IP Address, IP Mask, and Default Gateway fields of the IP Management window.

You can change the information in these fields. The mask identifies the bits that denote the network number in the IP address. When you use the mask to subnet a network, the mask is then referred to as a subnet mask. The broadcast address is reserved for sending messages to all hosts. The CPU sends traffic to an unknown IP address through the default gateway.

**Caution**

Changing the command switch IP address on this window ends your VSM session and any SNMP or Telnet sessions in progress. Restart the Cluster Manager by entering the new IP address in the browser **Location** field (Netscape Communicator) or **Address** field (Internet Explorer), as described in the [“Using VSM”](#) section on page 2-20.

## CLI: Assigning IP Information to the Switch

Beginning in privileged EXEC mode, follow these steps to enter the IP information:

|        | Command                                                   | Purpose                                                                                                                                                                              |
|--------|-----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>                                 | Enter global configuration mode.                                                                                                                                                     |
| Step 2 | <b>interface vlan 1</b>                                   | Enter interface configuration mode, and enter the VLAN to which the IP information is assigned.<br>VLAN 1 is the management VLAN, but you can configure any VLAN from IDs 1 to 1001. |
| Step 3 | <b>ip address</b> <i>ip_address</i><br><i>subnet_mask</i> | Enter the IP address and subnet mask.                                                                                                                                                |
| Step 4 | <b>exit</b>                                               | Return to global configuration mode.                                                                                                                                                 |
| Step 5 | <b>ip default-gateway</b> <i>ip_address</i>               | Enter the IP address of the default router.                                                                                                                                          |
| Step 6 | <b>end</b>                                                | Return to privileged EXEC mode.                                                                                                                                                      |
| Step 7 | <b>show running-config</b>                                | Verify that the information was entered correctly by displaying the running configuration. If the information is incorrect, repeat the procedure.                                    |



The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## CLI: Removing an IP Address

Use the following procedure to remove the IP information from a switch.



### Note

Using the **no ip address** command in configuration mode disables the IP protocol stack as well as removes the IP information. Cluster members without IP addresses rely on the IP protocol stack being enabled.

Beginning in privileged EXEC mode, follow these steps to remove an IP address:

|        | Command                                                         | Purpose                                                                          |
|--------|-----------------------------------------------------------------|----------------------------------------------------------------------------------|
| Step 1 | <b>clear ip address vlan 1</b><br><i>ip_address subnet_mask</i> | Remove the IP address and subnet mask.                                           |
| Step 2 | <b>end</b>                                                      | Return to privileged EXEC mode.                                                  |
| Step 3 | <b>show running-config</b>                                      | Verify that the information was removed by displaying the running configuration. |



### Caution

If you are removing the IP address through a Telnet session, your connection to the switch will be lost.

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## DHCP-Based Autoconfiguration

The DHCP provides configuration information to Internet hosts and internetworking devices. This protocol consists of two components: one for delivering configuration parameters from a DHCP server to a device and a

mechanism for allocating network addresses to devices. DHCP is built on a client-server model, where designated DHCP servers allocate network addresses and deliver configuration parameters to dynamically configured devices.

With DHCP-based autoconfiguration, your switch (DHCP client) can be automatically configured at startup with IP address information and a configuration file that it receives during DHCP-based autoconfiguration.

With DHCP-based autoconfiguration, no DHCP client-side configuration is required on your switch. However, you need to configure the DHCP server for various lease options. You might also need to configure a TFTP server, a Domain Name System (DNS) server, and possibly a relay device if the servers are on a different LAN than your switch. A relay device forwards broadcast traffic between two directly connected LANs. A router does not forward broadcast packets, but it forwards packets based on the destination IP address in the received packet. DHCP-based autoconfiguration replaces the BOOTP client functionality on your switch.

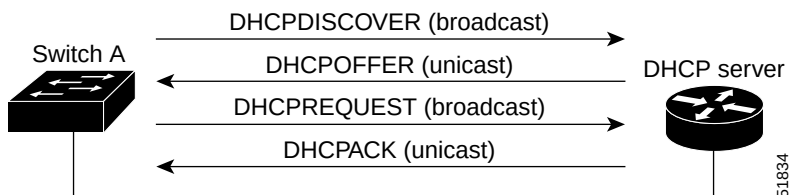
## DHCP Client Request Process

When you boot your switch, the DHCP client can be invoked and automatically request configuration information from a DHCP server under the following conditions:

- The configuration file is not present on the switch.
- The configuration file is present, but the IP address is not specified in it.
- The configuration file is present, the IP address is not specified in it, and the **service config** global configuration command is included. This command enables the autoloading of a configuration file from a network server.

Figure 4-14 shows the sequence of messages that are exchanged between the DHCP client and the DHCP server.

**Figure 4-14 DHCP Request for IP Information from a DHCP Server**



The client, Switch A, broadcasts a DHCPDISCOVER message to locate a DHCP server. The DHCP server offers configuration parameters (such as an IP address, subnet mask, gateway IP address, DNS IP address, a lease for the IP address, and so forth) to the client in a DHCPOFFER unicast message.

In a DHCPREQUEST broadcast message, the client returns a formal request for the offered configuration information to the DHCP server. The formal request is broadcast so that all other DHCP servers that received the DHCPDISCOVER broadcast message from the client can reclaim the IP addresses that they offered to the client.

The DHCP server confirms that the IP address has been allocated to the client by returning a DHCPACK unicast message to the client. With this message, the client and server are bound, and the client uses configuration information received from the server. The amount of information the switch receives depends on how you configure the DHCP server. For more information, see the [“Configuring the DHCP Server” section on page 4-32](#).

If the configuration parameters sent to the client in the DHCPOFFER unicast message by the DHCP server are invalid (a configuration error exists), the client returns a DHCPDECLINE broadcast message to the DHCP server.

The DHCP server sends the client a DHCPNAK denial broadcast message, which means the offered configuration parameters have not been assigned, an error has occurred during the negotiation of the parameters, or the client has been slow in responding to the DHCPOFFER message (the DHCP server assigned the parameters to another client) of the DHCP server.

A DHCP client might receive offers from multiple DHCP or BOOTP servers and can accept any one of the offers; however, the client usually accepts the first offer it receives. The offer from the DHCP server is not a guarantee that the IP address will be allocated to the client; however, the server usually reserves the address until the client has had a chance to formally request the address. If the switch accepts replies from a BOOTP server and configures itself, the switch will broadcast, instead of unicast, TFTP requests to obtain the switch configuration file.

## Configuring the DHCP Server

You should configure the DHCP servers with reserved leases that are bound to each switch by the switch hardware address. If the DHCP server does not support reserved leases, the switch can obtain different IP addresses and configuration files at different boot instances. You should configure the DHCP server with the following lease options:

- IP address of the client (required)
- Subnet mask of the client (required)
- DNS server IP address (required)
- Router IP address (default gateway address to be used by the switch) (required)
- TFTP server name (required)
- Boot filename (the name of the configuration file that the client needs) (recommended)
- Host name (optional)

If you do not configure the DHCP server with the lease options described earlier, then it replies to client requests with only those parameters that have available values. If the IP address and subnet mask are not in the reply, the switch is not configured. If the DNS server IP address, router IP address, or TFTP server name are not found, the switch might broadcast TFTP requests. Unavailability of other lease options does not affect autoconfiguration.



### Note

If the configuration file on the switch does not contain the IP address, the switch obtains its address, mask, gateway IP address, and host name from DHCP. If the **service config** global configuration command is specified in the configuration file, the switch receives the configuration file through TFTP requests. If the **service config** global configuration command and the IP address are both present in the configuration file, DHCP is not used, and the switch obtains the default configuration file by broadcasting TFTP requests.

The DHCP server can be on the same or a different LAN as the switch. If it is on a different LAN, the switch must be able to access it through a relay device. The DHCP server can be running on a UNIX or Linux operating system; however, the Windows NT operating system is not supported in this release.

For more information, see the [“Configuring the Relay Device” section on page 4-34](#). You must also set up the TFTP server with the switch configuration files; for more information, see the next section.

## Configuring the TFTP Server

The TFTP server must contain one or more configuration files in its base directory. The files can include the following:

- The configuration file named in the DHCP reply (the actual switch configuration file)
- The network-config or the cisco.net.cfg file (known as the default configuration files)
- The router-config or the cisco.rtr.cfg file (These files contain commands common to all switches. Normally, if the DHCP and TFTP servers are properly configured, these files are not accessed.)

You must specify the TFTP server name in the DHCP server lease database. You must also specify the TFTP server name-to-IP-address mapping in the DNS server database.

The TFTP server can be on the same or a different LAN as the switch. If it is on a different LAN, the switch must be able to access it through a relay device or a router. For more information, see the [“Configuring the Relay Device” section on page 4-34](#).

If the configuration filename is provided in the DHCP server reply, the configuration files for multiple switches can be spread over multiple TFTP servers. However, if the configuration filename is not provided, then the configuration files must reside on a single TFTP server.

## Configuring the DNS

The switch uses the DNS server to resolve the TFTP server name to a TFTP server IP address. You must configure the TFTP server name-to-IP address map on the DNS server. The TFTP server contains the configuration files for the switch.

You must configure the IP addresses of the DNS servers in the lease database of the DHCP server from where the DHCP replies will retrieve them. You can enter up to two DNS server IP addresses in the lease database.

The DNS server can be on the same or a different LAN as the switch. If it is on a different LAN, the switch must be able to access it through a relay device or router. For more information, see the [“Configuring the Relay Device” section on page 4-34](#).

## Configuring the Relay Device

You need to use a relay device if the DHCP, DNS, or TFTP servers are on a different LAN than the switch. You must configure this relay device to forward received broadcast packets on an interface to the destination host. This configuration ensures that broadcasts from the DHCP client can reach the DHCP, DNS, and TFTP servers and that broadcasts from the servers can reach the DHCP client.

If the relay device is a Cisco router, you enable IP routing (**ip routing** global configuration command) and configure it with helper addresses by using the **ip helper-address** interface configuration command.

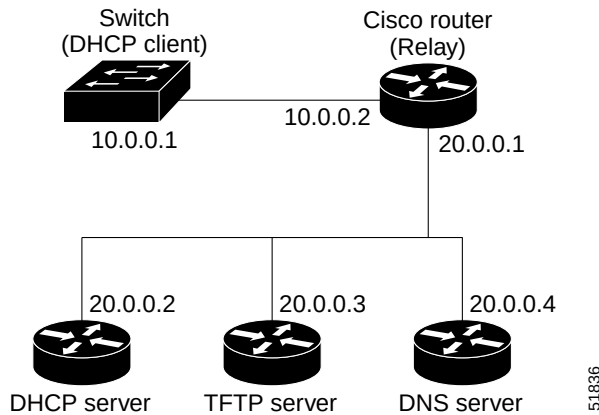
For example, in [Figure 4-15](#), you configure the router interfaces as follows:

On interface 10.0.0.2:

```
router(config-if)# ip helper-address 20.0.0.2
router(config-if)# ip helper-address 20.0.0.3
router(config-if)# ip helper-address 20.0.0.4
```

On interface 20.0.0.1

```
router(config-if)# ip helper-address 10.0.0.1
```

**Figure 4-15 Relay Device Used in Autoconfiguration**

51836

## Obtaining Configuration Files

Depending on the availability of the IP address and the configuration filename in the DHCP reserved lease, the switch obtains its configuration information in the following ways:

- The IP address and the configuration filename is reserved for the switch and provided in the DHCP reply (one-file read method).

The switch receives its IP address, subnet mask, and configuration filename from the DHCP server. It also receives a DNS server IP address and a TFTP server name. The switch sends a DNS request to the DNS server, specifying the TFTP server name, to obtain the TFTP server address. Then the switch sends a unicast message to the TFTP server to retrieve the named configuration file from the base directory of the server, and upon receipt, completes its boot-up process.

- Only the configuration filename is reserved for the switch. The IP address is dynamically allocated to the switch by the DHCP server (one-file read method).

The switch follows the same configuration process described above.

- Only the IP address is reserved for the switch and provided in the DHCP reply. The configuration filename is not provided (two-file read method).

The switch receives its IP address and subnet mask from the DHCP server. It also receives a DNS server IP address and a TFTP server name. The switch sends a DNS request to the DNS server, specifying the TFTP server name, to obtain the TFTP server address.

The switch sends a unicast message to the TFTP server to retrieve the `network-config` or `cisconet.cfg` default configuration file. (If the `network-config` file cannot be read, the switch reads the `cisconet.cfg` file.)

The default configuration file contains the host names-to-IP-address mapping for the switch. The switch fills its host table with the information in the file and obtains its host name. If the host name is not found in the file, the switch uses the host name in the DHCP reply. If the host name is not specified in the DHCP reply, the switch uses the default “Switch” as its host name.

After obtaining its host name from the default configuration file or the DHCP reply, the switch reads the configuration file that has the same name as its host name (*hostname-config* or *hostname.cfg*, depending on whether `network-config` or `cisconet.cfg` was read earlier) from the TFTP server. If the `cisconet.cfg` file is read, the filename of the host is truncated to eight characters.

If the switch cannot read the `network-config`, `cisconet.cfg`, or the host-name file, it reads the `router-config` file. If the switch cannot read the `router-config` file, it reads the `ciscotr.cfg` file.

**Note**

---

The switch broadcasts TFTP server requests if the TFTP server name is not obtained from the DHCP replies, if all attempts to read the configuration file through unicast transmissions fail, or if the TFTP server name cannot be resolved to an IP address.

---



## Example Configuration

Figure 4-16 shows a sample network for retrieving IP information using DHCP-based autoconfiguration.

**Figure 4-16 DHCP-Based Autoconfiguration Network Example**

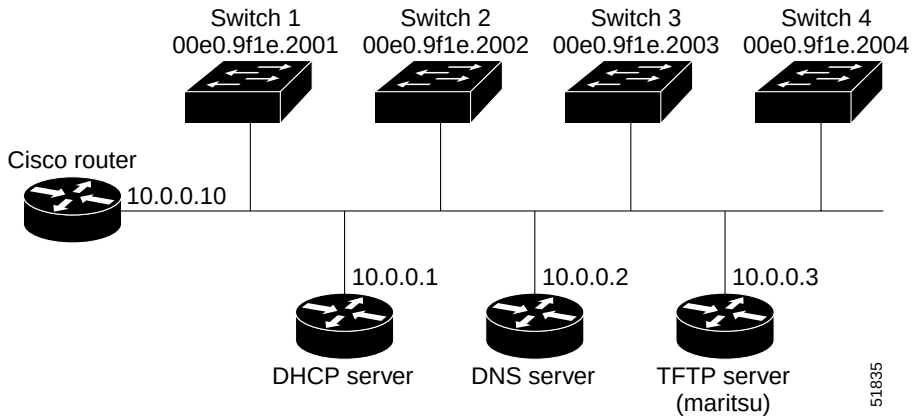


Table 4-3 shows the configuration of the reserved leases on the DHCP server.

**Table 4-3 DHCP Server Configuration**

|                                   | Switch-1            | Switch-2            | Switch-3            | Switch-4            |
|-----------------------------------|---------------------|---------------------|---------------------|---------------------|
| Binding key<br>(hardware address) | 00e0.9f1e.2001      | 00e0.9f1e.2002      | 00e0.9f1e.2003      | 00e0.9f1e.2004      |
| IP address                        | 10.0.0.21           | 10.0.0.22           | 10.0.0.23           | 10.0.0.24           |
| Subnet mask                       | 255.255.255.0       | 255.255.255.0       | 255.255.255.0       | 255.255.255.0       |
| Router address                    | 10.0.0.10           | 10.0.0.10           | 10.0.0.10           | 10.0.0.10           |
| DNS server address                | 10.0.0.2            | 10.0.0.2            | 10.0.0.2            | 10.0.0.2            |
| TFTP server name                  | maritsu or 10.0.0.3 | maritsu or 10.0.0.3 | maritsu or 10.0.0.3 | maritsu or 10.0.0.3 |

**Table 4-3 DHCP Server Configuration (continued)**

|                                                     | Switch-1      | Switch-2      | Switch-3      | Switch-4      |
|-----------------------------------------------------|---------------|---------------|---------------|---------------|
| Boot filename<br>(configuration<br>file) (optional) | switch1-confg | switch2-confg | switch3-confg | switch4-confg |
| Host name<br>(optional)                             | switch1       | switch2       | switch3       | switch4       |

### DNS Server Configuration

The DNS server maps the TFTP server name *maritsu* to IP address 10.0.0.3.

### TFTP Server Configuration (on UNIX)

The TFTP server base directory is set to `/tftpserver/work/`. This directory contains the `network-confg` file used in the two-file read method. This file contains the host name to be assigned to the switch based on its IP address. The base directory also contains a configuration file for each switch (`switch1-confg`, `switch2-confg`, and so forth) as shown in the following display:

```
prompt> cd /tftpserver/work/
prompt> ls
network-confg
switch1-confg
switch2-confg
switch3-confg
switch4-confg
prompt> cat network-confg
ip host switch1 10.0.0.21
ip host switch2 10.0.0.22
ip host switch3 10.0.0.23
ip host switch4 10.0.0.24
```

### DHCP Client Configuration

No configuration file is present on Switch 1 through Switch 4.

### Configuration Explanation

In [Figure 4-16](#), Switch 1 reads its configuration file as follows:

- It obtains its IP address 10.0.0.21 from the DHCP server.
- If no configuration filename is given in the DHCP server reply, Switch 1 reads the `network-confg` file from the base directory of the TFTP server.

- It adds the contents of the network-config file to its host table.
- It reads its host table by indexing its IP address 10.0.0.21 to its host name (switch1).
- It reads the configuration file that corresponds to its host name; for example, it reads switch1-config from the TFTP server.

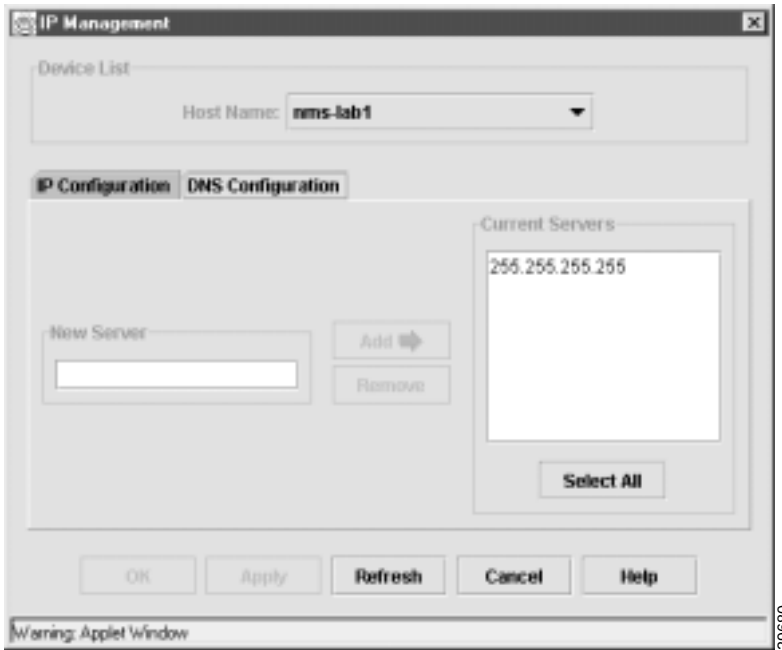
Switches 2 through 4 retrieve their configuration files and IP addresses in the same way.

## Specifying a Domain Name and Configuring the DNS

Each unique Internet Protocol (IP) address can have a host name associated with it. The IOS software maintains a cache of host name-to-address mappings for use by the EXEC mode **connect**, **telnet**, **ping**, and related Telnet support operations. This cache speeds the process of converting names to addresses.

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, the File Transfer Protocol (FTP) system for example, is identified as *ftp.cisco.com*.

To keep track of domain names, IP has defined the concept of a domain name server (DNS), whose job is to hold a cache (or database) of names mapped to IP addresses. To map domain names to IP addresses, you must first identify the host names and then specify a name server and enable the DNS, the Internet's global naming scheme that uniquely identifies network devices.

**Figure 4-17 DNS Configuration**

Domain name servers handle name and address resolution.

## Specifying the Domain Name

You can specify a default domain name that the software uses to complete domain name requests. You can specify either a single domain name or a list of domain names. When you specify a domain name, any IP host name without a domain name will have that domain name appended to it before being added to the host table.

To specify a domain name, enter the name into the Domain Name field of the IP Configuration tab of the IP Management window (Figure 4-17), and click **OK**. Do not include the initial period that separates an unqualified name (names without a dotted-decimal domain name) from the domain name.

You can also configure the DNS name by using the CLI. The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## Specifying a Name Server

You can specify up to six hosts that can function as a name server to supply name information for the DNS. Enter the IP address into the New Server field, and click **Add**.

## Enabling the DNS

If your network devices require connectivity with devices in networks for which you do not control name assignment, you can assign device names that uniquely identify your devices within the entire internetwork. The Internet's global naming scheme, the DNS, accomplishes this task. This service is enabled by default.

# Configuring SNMP

Use the SNMP Management window ([Figure 4-18](#)) to configure your switch for SNMP management. If your switch is part of a cluster, the clustering software can change SNMP parameters (such as host names) when the cluster is created. If you are configuring a cluster for SNMP, see the [“Configuring SNMP for a Cluster” section on page 3-59](#).

You can use this window to perform the following tasks:

- Disabling and enabling SNMP.
- Entering general information about the switch.
- Entering community strings that serve as passwords for SNMP messages.
- Entering trap managers and their community strings to receive traps (alerts) about switch activity.
- Setting the classes of traps a trap manager receives.

To display this window, select **System > SNMP Configuration** from the menu bar.

## Disabling and Enabling SNMP

SNMP is enabled by default and must be enabled for Cluster Management features to work properly. If you deselect **Enable SNMP** and click **Apply**, SNMP is disabled, and the SNMP parameters are disabled. For information on SNMP and Cluster Management, see [“Managing Cluster Switches Through SNMP” section on page 2-37](#).

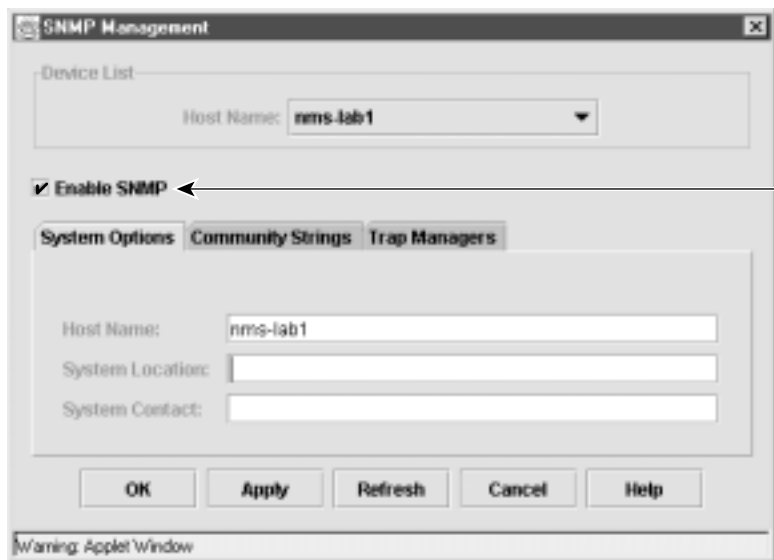
SNMP is always enabled for 1900 and 2820 switches.

## Entering Community Strings

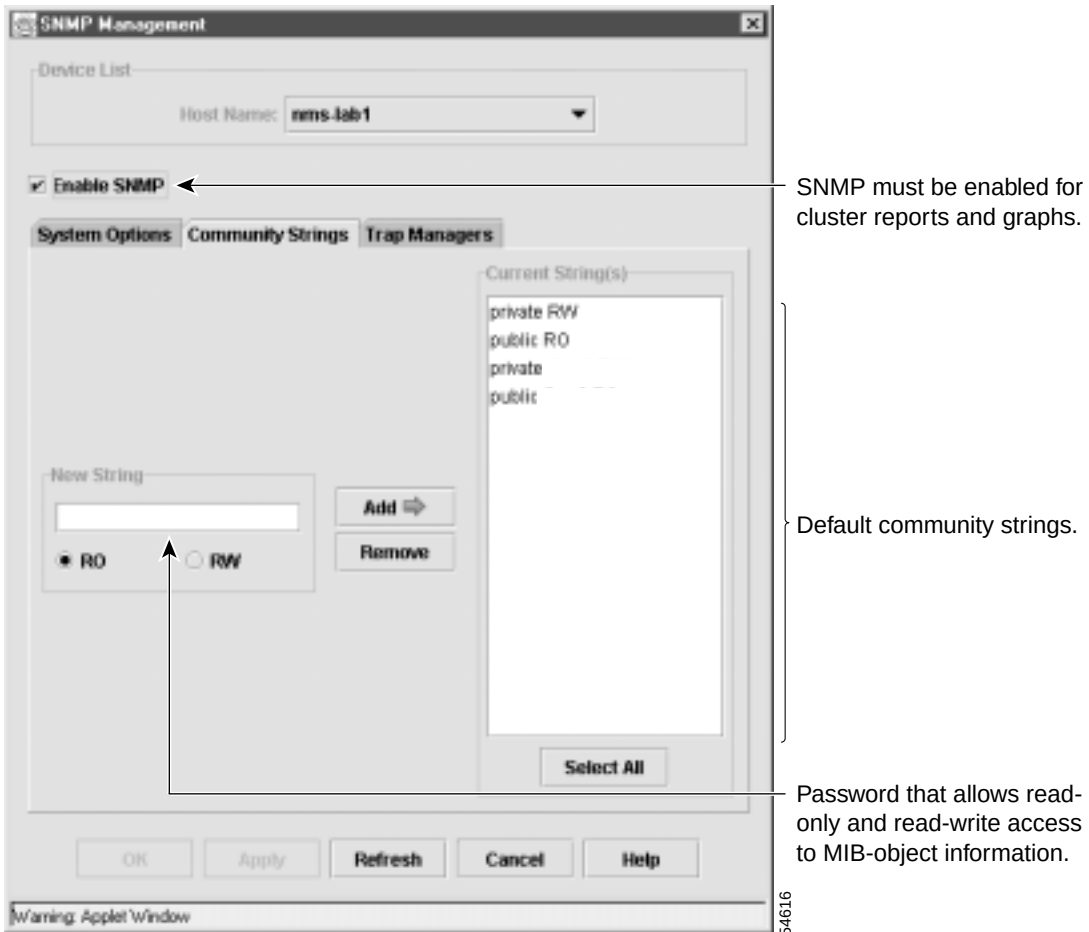
Community strings serve as passwords for SNMP messages to permit access to the agent on the switch. If you are entering community strings for a cluster member, see the [“Configuring Community Strings for Cluster Switches” section on page 3-60](#). You can enter community strings with the following characteristics:

- |                 |                                                                                            |
|-----------------|--------------------------------------------------------------------------------------------|
| Read-only (RO)  | Requests accompanied by the string can display MIB-object information.                     |
| Read-write (RW) | Requests accompanied by the string can display MIB-object information and set MIB objects. |

Use the Community Strings tab ([Figure 4-19](#)) to add and remove community strings. You can also use the CLI to configure SNMP community strings. The [“Finding More Information About IOS Commands” section on page 4-1](#) contains the path to the complete IOS documentation.

**Figure 4-18 SNMP Management—System Options**

SNMP must be enabled for cluster reports and graphs.

**Figure 4-19 SNMP Configuration—Community Strings**

## Adding Trap Managers

A trap manager is a management station that receives and processes traps. When you configure a trap manager, community strings for each member switch must be unique. If a member switch has an IP address assigned to it, the management



station accesses the switch by using its assigned IP address. Use the Trap Managers tab ([Figure 4-20](#)) to configure trap managers and enter trap manager community strings.

By default, no trap manager is defined, and no traps are issued. Select a check box to enable one of the following classes of traps:

|                 |                                                                                             |
|-----------------|---------------------------------------------------------------------------------------------|
| Config          | Generate traps whenever the switch configuration changes.                                   |
| SNMP            | Generate the supported SNMP traps.                                                          |
| TTY             | Generate traps when the switch starts a management console CLI session.                     |
| VLAN membership | Generate a trap for each VLAN Membership Policy Server (VMPS) change.                       |
| VTP             | Generate a trap for each VLAN Trunk Protocol (VTP) change.                                  |
| C2900/C3500     | Generate the switch-specific traps. These traps are in the private enterprise-specific MIB. |

**Figure 4-20 SNMP Management—Trap Managers**

29700

## CLI: Adding a Trap Manager

Beginning in privileged EXEC mode, follow these steps to add a trap manager and community string:

|        | Command                                                           | Purpose                                                                                    |
|--------|-------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| Step 1 | <b>config terminal</b>                                            | Enter global configuration mode.                                                           |
| Step 2 | <b>snmp-server host 172.2.128.263 traps1 snmp vlan-membership</b> | Enter the trap manager IP address, community string, and the traps to generate.            |
| Step 3 | <b>end</b>                                                        | Return to privileged EXEC mode.                                                            |
| Step 4 | <b>show running-config</b>                                        | Verify that the information was entered correctly by displaying the running configuration. |

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## Managing the ARP Table

To communicate with a device (on Ethernet, for example), the software first must determine the 48-bit MAC or local data link address of that device. The process of determining the local data link address from an IP address is called *address resolution*.

The Address Resolution Protocol (ARP) associates a host IP address with the corresponding media or MAC addresses and VLAN ID. Taking an IP address as input, ARP determines the associated MAC address. Once a MAC address is determined, the IP-MAC address association is stored in an ARP cache for rapid retrieval. Then the IP datagram is encapsulated in a link-layer frame and sent over the network. Encapsulation of IP datagrams and ARP requests and replies on IEEE 802 networks other than Ethernet is specified by the Subnetwork Access Protocol (SNAP). By default, standard Ethernet-style ARP encapsulation (represented by the **arpa** keyword) is enabled on the IP interface.

Use the ARP Table window ([Figure 4-21](#)) to display the table and change the timeout value.

To display this window, select **System > ARP Table** from the menu bar. ARP entries added manually to the table do not age and must be manually removed.

You can manually add entries to the ARP Table by using the CLI; however, these entries do not age and must be manually removed. The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

**Figure 4-21 ARP Table**

ARP

Device List

Host Name: 2950-24-146 ▼

ARP Table

| Protocol | Address        | Age (min) | Hardware Ad... | Type | Interface |
|----------|----------------|-----------|----------------|------|-----------|
| Internet | 172.20.139.... | -         | 0001.96e4.e... | ARPA | VLAN1     |
| Internet | 172.20.139.... | 0         | 0001.96e4.e... | ARPA | VLAN1     |
| Internet | 172.20.139.... | 0         | 0030.19c6.5... | ARPA | VLAN1     |

Remove All

ARP Cache Timeout Value (1-4294967 sec): 1

OK Apply Refresh Cancel Help

Warning: Applet Window

# Managing the MAC Address Tables

Use the Address Management window (Figure 4-23) to manage the MAC address tables that the switch uses to forward traffic between ports. All MAC addresses in the address tables are associated with one or more ports. These MAC tables include the following types of addresses:

- Dynamic address: a source MAC address that the switch learns and then drops when it is not in use.
- Secure address: a manually entered unicast address that is usually associated with a secure port. Secure addresses do not age.
- Static address: a manually entered unicast or multicast address that does not age and that is not lost when the switch resets.

To display this window, select **Security > Address Management** from the menu bar.

The address tables list the destination MAC address and the associated VLAN ID, module, and port number associated with the address. Figure 4-22 shows an example list of addresses as they would appear in the dynamic, secure, or static address table.

**Figure 4-22 Contents of the Address Table**

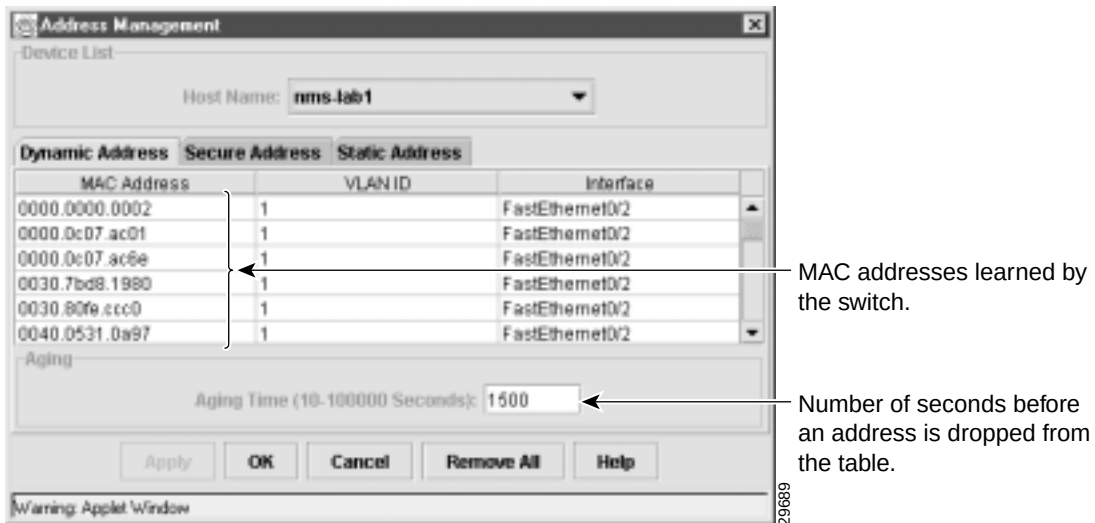
|                |   |                 |
|----------------|---|-----------------|
| 0010.07a0.6bc1 | 1 | FastEthernet0/1 |
| 0010.0b39.b901 | 1 | FastEthernet0/2 |
| 0010.7b00.1900 | 1 | FastEthernet0/3 |
| 0010.7b00.1901 | 1 | FastEthernet0/3 |
| 0060.5c21.c875 | 1 | FastEthernet0/1 |

## MAC Addresses and VLANs

All addresses are associated with a VLAN. An address can exist in more than one VLAN and have different destinations in each. Multicast addresses, for example, could be forwarded to port 1 in VLAN 1 and ports 9, 10, and 11 in VLAN 5.

Each VLAN maintains its own logical address table. A known address in one VLAN is unknown in another until it is learned or statically associated with a port in the other VLAN. An address can be secure in one VLAN and dynamic in another. Addresses that are statically entered in one VLAN must be static addresses in all other VLANs.

**Figure 4-23 Address Management—Dynamic Address**



## Changing the Address Aging Time

Dynamic addresses are source MAC addresses that the switch learns and then drops when they are not in use. Use the Aging Time field to define how long the switch retains unseen addresses in the table. This parameter applies to all VLANs.

## CLI: Configuring the Aging Time

Setting too short an aging time can cause addresses to be prematurely removed from the table. Then when the switch receives a packet for an unknown destination, it floods the packet to all ports in the same VLAN as the receiving port. This unnecessary flooding can impact performance. Setting too long an aging time can cause the address table to be filled with unused addresses; it can cause delays in establishing connectivity when a workstation is moved to a new port.

Beginning in privileged EXEC mode, follow these steps to configure the dynamic address table aging time.

|        | Command                                               | Purpose                                                                                                                                |
|--------|-------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>                             | Enter global configuration mode.                                                                                                       |
| Step 2 | <b>mac-address-table aging-time</b><br><i>seconds</i> | Enter the number of seconds that dynamic addresses are to be retained in the address table. You can enter a number from 10 to 1000000. |
| Step 3 | <b>end</b>                                            | Return to privileged EXEC mode.                                                                                                        |
| Step 4 | <b>show mac-address-table</b><br><b>aging-time</b>    | Verify your entry.                                                                                                                     |

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## CLI: Removing Dynamic Address Entries

Beginning in privileged EXEC mode, follow these steps to remove a dynamic address entry:

|        | Command                                               | Purpose                                                             |
|--------|-------------------------------------------------------|---------------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>                             | Enter global configuration mode.                                    |
| Step 2 | <b>no mac-address-table dynamic</b><br><i>hw-addr</i> | Enter the MAC address to be removed from dynamic MAC address table. |
| Step 3 | <b>end</b>                                            | Return to privileged EXEC mode.                                     |
| Step 4 | <b>show mac-address-table</b>                         | Verify your entry.                                                  |

You can remove all dynamic entries by using the **clear mac-address-table dynamic** command in privileged EXEC mode.

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

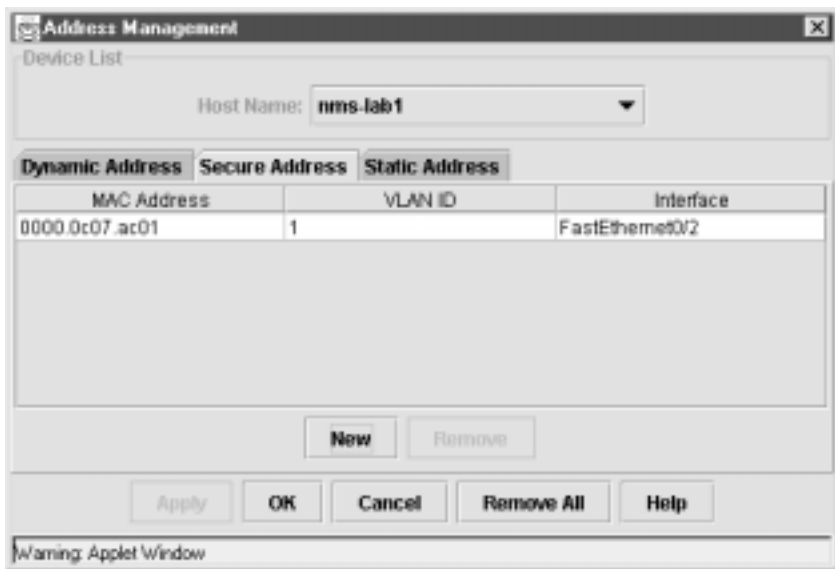
## Adding Secure Addresses

The secure address table contains secure MAC addresses and their associated ports and VLANs. A secure address is a manually entered unicast address that is forwarded to only one port per VLAN. If you enter an address that is already assigned to another port, the switch reassigns the secure address to the new port.

You can enter a secure port address even when the port does not yet belong to a VLAN. When the port is later assigned to a VLAN, packets destined for that address are forwarded to the port.

You can use the Secure Address tab ([Figure 4-24](#)) to remove individual secure addresses or a group of them. To display this window, click the **Secure Address** tab on the Address Management window. Click the **New** button to display the New Address window ([Figure 4-25](#)), and enter a new secure address.



**Figure 4-24 Address Management—Secure Address Tab**

29701

After you have entered the secure address, select **Security > Port Security** from the menu bar to secure the port by using the Port Security window.

Figure 4-25 New Secure Address

Enter a secure MAC address for a port. Secure the port on the Port Security Page.

29690

## CLI: Adding Secure Addresses

Beginning in privileged EXEC mode, follow these steps to add a secure address:

|        | Command                                                                                   | Purpose                                                      |
|--------|-------------------------------------------------------------------------------------------|--------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>                                                                 | Enter global configuration mode.                             |
| Step 2 | <b>mac-address-table secure</b><br><i>hw-addr interface</i><br><b>vlan</b> <i>vlan-id</i> | Enter the MAC address, its associated port, and the VLAN ID. |
| Step 3 | <b>end</b>                                                                                | Return to privileged EXEC mode.                              |
| Step 4 | <b>show mac-address-table secure</b>                                                      | Verify your entry.                                           |

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## CLI: Removing Secure Addresses

Beginning in privileged EXEC mode, follow these steps to remove a secure address:

|        | Command                                                           | Purpose                                                                           |
|--------|-------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>                                         | Enter global configuration mode.                                                  |
| Step 2 | <b>no mac-address-table secure</b><br><i>hw-addr vlan vlan-id</i> | Enter the secure MAC address, its associated port, and the VLAN ID to be removed. |
| Step 3 | <b>end</b>                                                        | Return to privileged EXEC mode.                                                   |
| Step 4 | <b>show mac-address-table secure</b>                              | Verify your entry.                                                                |

You can remove all secure addresses by using the **clear mac-address-table secure** command in privileged EXEC mode.

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## Adding and Removing Static Addresses

A static address has the following characteristics:

- It is manually entered in the address table and must be manually removed.
- It can be a unicast or multicast address.
- It does not age and is retained when the switch restarts.

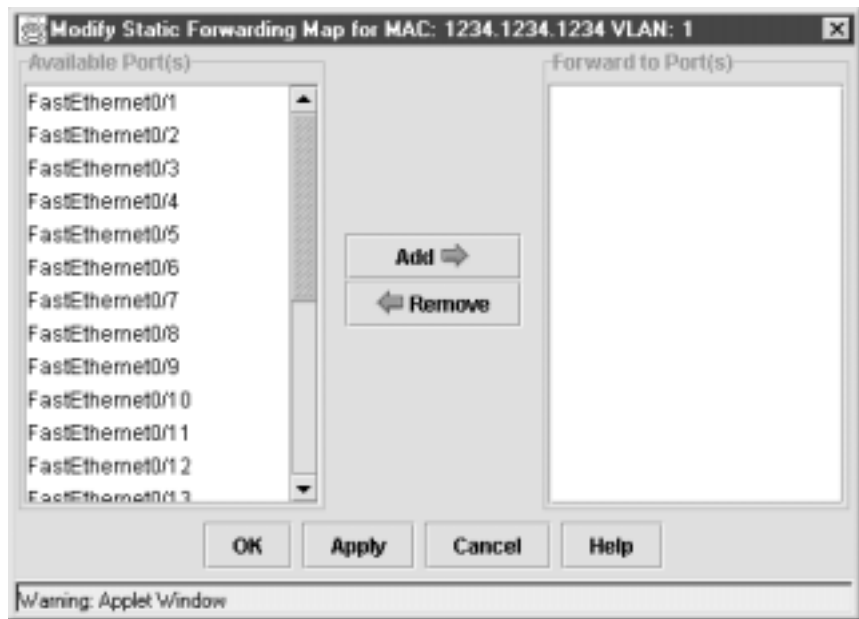
By clicking the **Static Address** tab on the Address Management window (Figure 4-23), you can add and remove static addresses. You can also define the forwarding behavior for the static address. Click **Forwarding** to display the Modify Static Forwarding window (Figure 4-26).

On the Modify Static Forwarding window, you determine how a port that receives a packet forwards it to another port for transmission. Because all ports are associated with at least one VLAN, the switch acquires the VLAN ID for the address from the ports that you select on the forwarding map.

The Available Port(s) column lists the ports where a static address is received. The Forward to Port(s) column lists the ports that the address with the static address can be forwarded to. Select a row, and click **Modify** to change the entries for an address.

A static address in one VLAN must be a static address in other VLANs. A packet with a static address that arrives on a VLAN where it has not been statically entered is flooded to all ports and not learned.

**Figure 4-26 Static Address Forwarding**



## Configuring Static Addresses for EtherChannel Port Groups

Follow these rules if you are configuring a static address to forward to ports in an EtherChannel port group:

- For default source-based port groups, configure the static address to forward to *all ports* in the port group to eliminate lost packets.
- For destination-based port groups, configure the address to forward to *only one port* in the port group to avoid the transmission of duplicate packets.

## CLI: Adding Static Addresses

Static addresses are entered in the address table with an *out-port-list* and a VLAN ID, if needed. Packets are forwarded to ports listed in the out-port-list.



### Note

If the in-port and out-port-list parameters are all access ports in a single VLAN, you can omit the VLAN ID. In this case, the switch recognizes the VLAN as that associated with the in-port VLAN. Otherwise, you must supply the VLAN ID.

Beginning in privileged EXEC mode, follow these steps to add a static address:

|        | Command                                                                                                 | Purpose                                                                                                                                                                                                                                         |
|--------|---------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>                                                                               | Enter global configuration mode.                                                                                                                                                                                                                |
| Step 2 | <b>mac-address-table static</b><br><i>hw-addr interface out-port-list</i><br><b>vlan</b> <i>vlan-id</i> | Enter the MAC address, the ports to which it can be forwarded, and the VLAN ID of those ports. For unicast static addresses, only one output port can be specified. For multicast static addresses, more than one output port can be specified. |
| Step 3 | <b>end</b>                                                                                              | Return to privileged EXEC mode.                                                                                                                                                                                                                 |
| Step 4 | <b>show mac-address-table static</b>                                                                    | Verify your entry.                                                                                                                                                                                                                              |

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## CLI: Removing Static Addresses

Beginning in privileged EXEC mode, follow these steps to remove a static address:

|        | Command                                                                                                    | Purpose                                                                                              |
|--------|------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>                                                                                  | Enter global configuration mode.                                                                     |
| Step 2 | <b>no mac-address-table static</b><br><i>hw-addr interface out-port-list</i><br><b>vlan</b> <i>vlan-id</i> | Enter the static MAC address, the ports to which it can be forwarded, and the VLAN ID to be removed. |
| Step 3 | <b>end</b>                                                                                                 | Return to privileged EXEC mode.                                                                      |
| Step 4 | <b>show mac-address-table static</b>                                                                       | Verify your entry.                                                                                   |

You can remove all secure addresses by using the **clear mac-address-table static** command in privileged EXEC mode.

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## Enabling Port Security

Secure ports restrict a port to a user-defined group of stations. When you assign secure addresses to a secure port, the switch does not forward any packets with source addresses outside the group of addresses you have defined. If you define the address table of a secure port to contain only one address, the workstation or server attached to that port is guaranteed the full bandwidth of the port.

Use the Port Security window ([Figure 4-27](#)) to enable port security on a port and to define the actions to take place when a security violation occurs. As part of securing the port, you can also define the size of the address table for the port.

To display this window, select **Security > Port Security** from the menu bar. To modify port-security parameters for several ports at once, select the rows by using the mouse, and click **Modify** to display the Port Security Configuration window ([Figure 4-28](#)).

Secure ports generate address-security violations under the following conditions:

- The address table of a secure port is full and the address of an incoming packet is not found in the table.
- An incoming packet has a source address assigned as a secure address on another port.

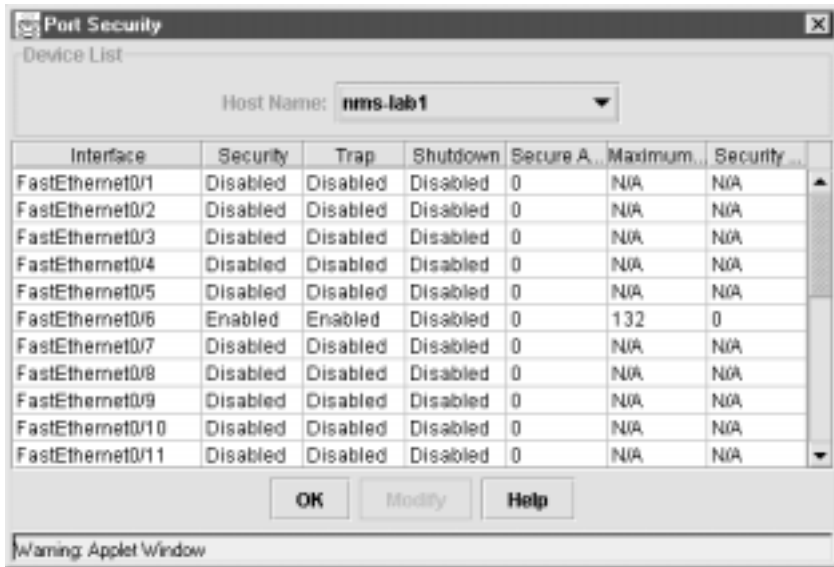
Limiting the number of devices that can connect to a secure port has the following advantages:

- Dedicated bandwidth—If the size of the address table is set to 1, the attached device is guaranteed the full bandwidth of the port.
- Added security—Unknown devices cannot connect to the port.

The following fields validate port security or indicate security violations:

|                  |                                                                                                       |
|------------------|-------------------------------------------------------------------------------------------------------|
| Interface        | Port to secure.                                                                                       |
| Security         | Enable port security on the port.                                                                     |
| Trap             | Issue a trap when an address-security violation occurs.                                               |
| Shutdown Port    | Disable the port when an address-security violation occurs.                                           |
| Secure Addresses | Number of addresses in the address table for this port. Secure ports have at least one in this field. |
| Max Addresses    | Number of addresses that the address table for the port can contain.                                  |
| Security Rejects | The number of unauthorized addresses seen on the port.                                                |

For the restrictions that apply to secure ports, see the [“Managing Configuration Conflicts” section on page 4-2](#).

**Figure 4-27 Port Security**

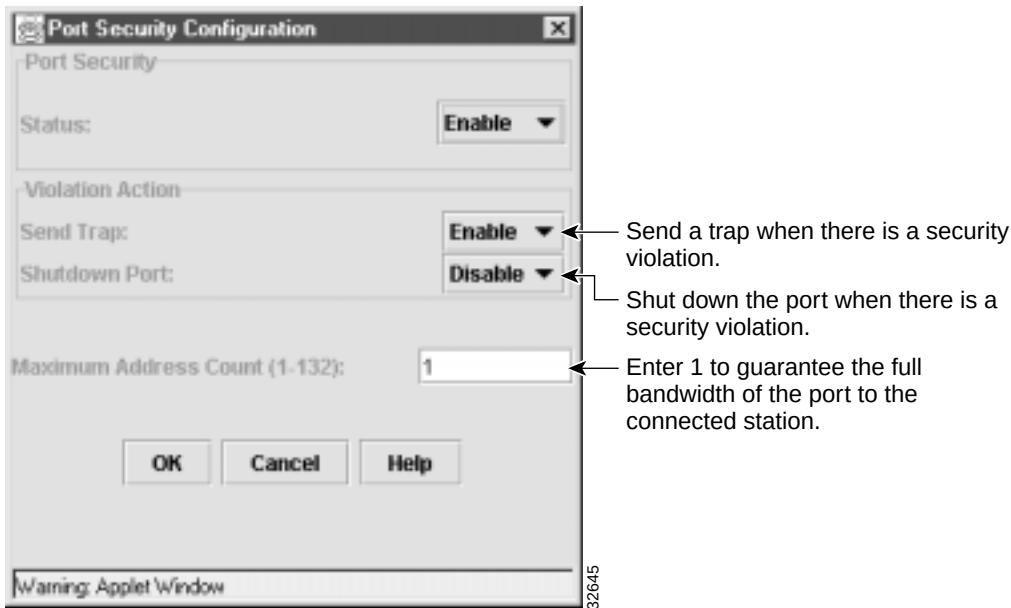
32644

## Defining the Maximum Secure Address Count

A secure port can have from 1 to 132 associated secure addresses. Setting one address in the MAC address table for the port ensures that the attached device has the full bandwidth of the port.



Figure 4-28 Port Security Configuration Pop-up



## CLI: Enabling Port Security

Beginning in privileged EXEC mode, follow these steps to enable port security.

|        | Command                              | Purpose                                                             |
|--------|--------------------------------------|---------------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>            | Enter global configuration mode.                                    |
| Step 2 | <b>interface <i>interface</i></b>    | Enter interface configuration mode for the port you want to secure. |
| Step 3 | <b>port security max-mac-count 1</b> | Secure the port and set the address table to one address.           |
| Step 4 | <b>port security action shutdown</b> | Set the port to shutdown when a security violation occurs.          |
| Step 5 | <b>end</b>                           | Return to privileged EXEC mode.                                     |
| Step 6 | <b>show port security</b>            | Verify the entry.                                                   |

[“Finding More Information About IOS Commands” section on page 4-1](#) contains the path to the complete IOS documentation.

## CLI: Disabling Port Security

Beginning in privileged EXEC mode, follow these steps to disable port security.

|        | Command                           | Purpose                                                               |
|--------|-----------------------------------|-----------------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>         | Enter global configuration mode.                                      |
| Step 2 | <b>interface</b> <i>interface</i> | Enter interface configuration mode for the port you want to unsecure. |
| Step 3 | <b>no port security</b>           | Disable port security                                                 |
| Step 4 | <b>end</b>                        | Return to privileged EXEC mode.                                       |
| Step 5 | <b>show port security</b>         | Verify the entry                                                      |

The [“Finding More Information About IOS Commands” section on page 4-1](#) contains the path to the complete IOS documentation.

## Configuring the Cisco Discovery Protocol

Use the Cisco IOS command-line interface and Cisco Discovery Protocol (CDP) to enable CDP for the switch, set global CDP parameters, and display information about neighboring Cisco devices.

CDP enables the Cluster Management Suite to display a graphical view of the network. For example, the switch uses CDP to find cluster candidates and maintain information about cluster members and other devices up to three cluster-enabled devices away from the command switch.

If necessary, you can configure CDP to discover switches running the Cluster Management Suite up to seven devices away from the command switch. Devices that do not run clustering software display as edge devices, and no device connected to them can be discovered by CDP.

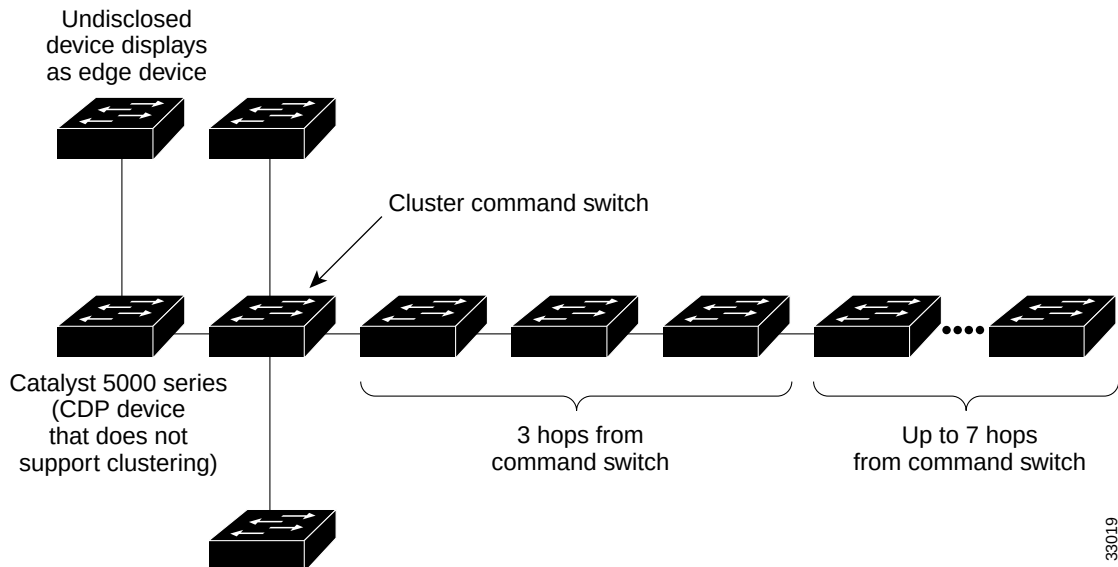
**Note**

Creating and maintaining switch clusters is based on the regular exchange of CDP messages. Disabling CDP can interrupt cluster discovery. For more information on the role that CDP plays in clustering, see the [“Automatically Discovering Cluster Candidates”](#) section on page 3-6.

## CLI: Configuring CDP for Extended Discovery

You can change the default configuration of CDP on the command switch to continue discovering devices up to seven *hops* away. [Figure 4-29](#) shows a command switch that can discover candidates up to seven devices away from it. [Figure 4-29](#) also shows the command switch connected to a Catalyst 5000 series switch. Because the Catalyst 5000 is a CDP device that does not support clustering, the command switch cannot learn about cluster candidate switches connected to it, even if they are running the Cluster Management Suite.

**Figure 4-29 Discovering Cluster Candidates via CDP**



Beginning in privileged EXEC mode, follow these steps to configure the number of hops that CDP discovers.

|        | Command                                             | Purpose                                                                                                 |
|--------|-----------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>                           | Enter global configuration mode.                                                                        |
| Step 2 | <b>cluster discovery hop-count</b><br><i>number</i> | Enter the number of hops that you want CDP to search for cluster candidates.                            |
| Step 3 | <b>end</b>                                          | Return to privileged EXEC mode.                                                                         |
| Step 4 | <b>show running-config</b>                          | Verify the change by displaying the running configuration file. The hop count is displayed in the file. |

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## IGMP Snooping

Internet Group Management Protocol (IGMP) snooping constrains the flooding of multicast traffic by dynamically configuring the interfaces so that multicast traffic is forwarded only to those interfaces associated with IP multicast devices. The LAN switch snoops on the IGMP traffic between the host and the router and keeps track of multicast groups and member ports. When the switch receives an IGMP join report from a host for a particular multicast group, the switch adds the host port number to the associated multicast forwarding table entry. When it receives an IGMP Leave Group message from a host, it removes the host port from the table entry. After it relays the IGMP queries from the multicast router, it deletes entries periodically if it does not receive any IGMP membership reports from the multicast clients.

When IGMP snooping is enabled, the multicast router sends out periodic IGMP general queries to all VLANs. The switch responds to the router queries with only one join request per MAC multicast group, and the switch creates one entry per VLAN in the Layer 2 forwarding table for each MAC group from which it receives an IGMP join request. All hosts interested in this multicast traffic send join requests and are added to the forwarding table entry.

Layer 2 multicast groups learned through IGMP snooping are dynamic. However, you can statically configure MAC multicast groups by using the **ip igmp snooping vlan static** command. If you specify group membership for a multicast group address statically, your setting supersedes any automatic manipulation by IGMP snooping. Multicast group membership lists can consist of both user-defined and IGMP snooping-learned settings.

Catalyst 2950 switches support a maximum of 255 IP multicast groups and support both IGMP version 1 and IGMP version 2.

If a port spanning-tree, a port group, or a VLAN ID change occurs, the IGMP snooping-learned multicast groups from this port on the VLAN are purged.

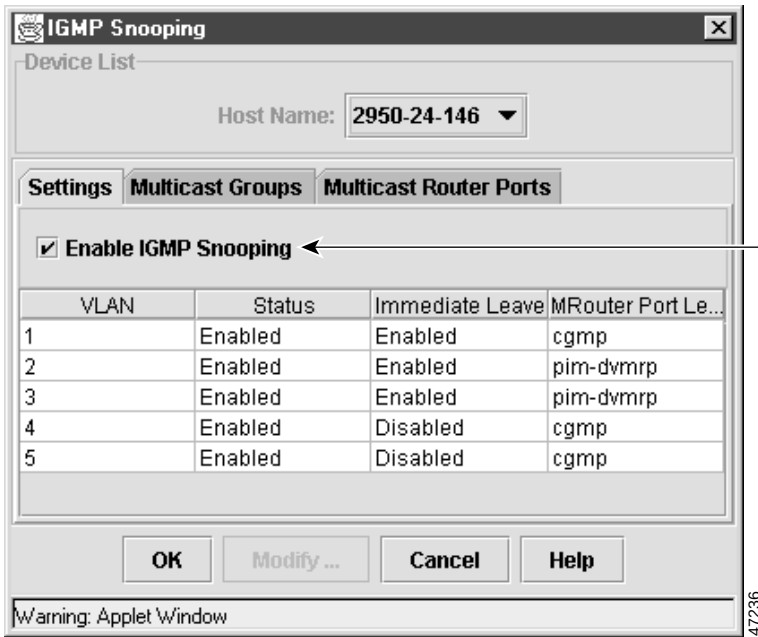
In the IP multicast-source-only environment, the switch learns the IP multicast group from the IP multicast data stream and only forwards traffic to the multicast router ports.

Use the IGMP Snooping window ([Figure 4-30](#)) to enable the IGMP snooping feature. To display this window, select **Device > IGMP Snooping** from the menu bar.

You can use this window to perform the following tasks:

- Enable or disable IGMP snooping
- Enable or disable Immediate-Leave processing
- Join or leave a multicast group
- Configure a multicast router

Figure 4-30 IGMP Snooping



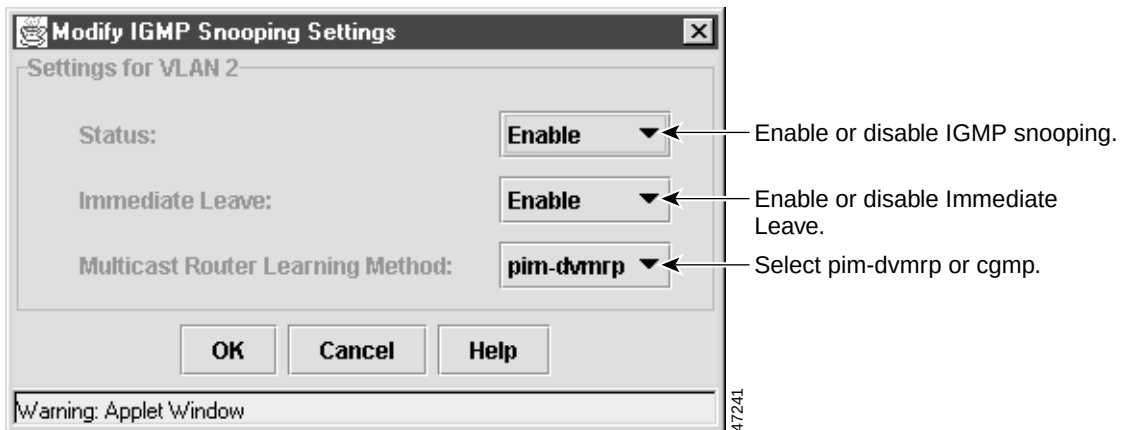
IGMP snooping is enabled by default. Deselect this if you want to disable IGMP snooping on the entire device.

## Enabling or Disabling IGMP Snooping

By default, IGMP snooping is globally enabled on the switch. When globally enabled or disabled, it is also enabled or disabled in all existing VLAN interfaces. By default, IGMP snooping is enabled on all VLANs, but it can be enabled and disabled on a per-VLAN basis.

Global IGMP snooping overrides the per-VLAN IGMP snooping capability. If global snooping is disabled, you cannot enable VLAN snooping. If global snooping is enabled, you can enable or disable snooping on a VLAN basis.

To modify the IGMP snooping settings on a per-VLAN basis, select a row, and click **Modify**. You can modify the settings as shown in [Figure 4-31](#).

**Figure 4-31** Modify the IGMP Snooping Settings

## CLI: Enabling or Disabling IGMP Snooping

Beginning in privileged EXEC mode, follow these steps to enable IGMP snooping globally on the switch:

|        | Command                                   | Purpose                                                          |
|--------|-------------------------------------------|------------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>                 | Enter global configuration mode.                                 |
| Step 2 | <b>ip igmp snooping</b>                   | Globally enable IGMP snooping in all existing VLAN interfaces.   |
| Step 3 | <b>end</b>                                | Return to privileged EXEC mode.                                  |
| Step 4 | <b>show ip igmp snooping</b>              | Display snooping configuration.                                  |
| Step 5 | <b>copy running-config startup-config</b> | (Optional) Save your configuration to the startup configuration. |

To globally disable IGMP snooping on all existing VLAN interfaces, use the **no ip igmp snooping** global command.

Beginning in privileged EXEC mode, follow these steps to enable IGMP snooping on a VLAN interface:

|        | Command                                            | Purpose                                                                                 |
|--------|----------------------------------------------------|-----------------------------------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>                          | Enter global configuration mode.                                                        |
| Step 2 | <b>ip igmp snooping vlan <i>vlan_id</i></b>        | Enable IGMP snooping on the VLAN interface.                                             |
| Step 3 | <b>end</b>                                         | Return to privileged EXEC mode.                                                         |
| Step 4 | <b>show ip igmp snooping [vlan <i>vlan_id</i>]</b> | Display snooping configuration.<br>(Optional) <i>vlan_id</i> is the number of the VLAN. |
| Step 5 | <b>copy running-config startup-config</b>          | (Optional) Save your configuration to the startup configuration.                        |

To disable IGMP snooping on a VLAN interface, use the global configuration command **no ip igmp snooping vlan *vlan\_id*** for the specified VLAN number (for example, *vlan1*).

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## CLI: Enabling IGMP Immediate-Leave Processing

When you enable IGMP Immediate-Leave processing, the switch immediately removes a port from the IP multicast group when it detects an IGMP version 2 leave message on that port. Immediate-Leave processing allows the switch to remove an interface that sends a leave message from the forwarding table without first sending out group specific queries to the interface. You should use the Immediate-Leave feature only when there is only a single receiver present on every port in the VLAN.



Beginning in privileged EXEC mode, follow these steps to enable IGMP Immediate-Leave processing:

|        | Command                                                     | Purpose                                                       |
|--------|-------------------------------------------------------------|---------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>                                   | Enter global configuration mode.                              |
| Step 2 | <b>ip igmp snooping vlan <i>vlan_id</i> immediate-leave</b> | Enable IGMP Immediate-Leave processing on the VLAN interface. |
| Step 3 | <b>end</b>                                                  | Return to privileged EXEC mode.                               |

To disable Immediate-Leave processing, follow Steps 1 and 2 to enter interface configuration mode, and use the command **no ip igmp snooping vlan *vlan\_id* immediate-leave**.

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## Setting the Snooping Method

Multicast-capable router ports are added to the forwarding table for every IP multicast entry. The switch learns of such ports through one of these methods:

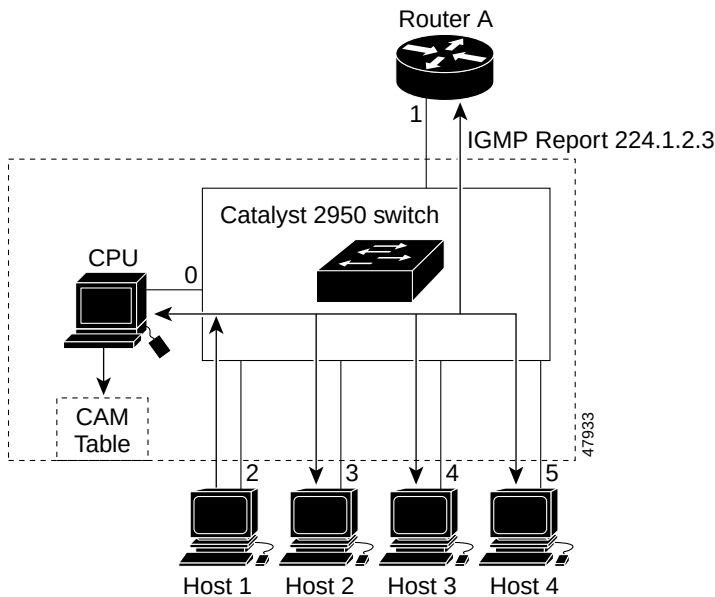
- Snooping on PIM and DVMRP packets
- Listening to CGMP self-join packets from other routers
- Statically connecting to a multicast router port with the **ip igmp snooping mrouter** command

You can configure the switch to either snoop on Protocol Independent Multicast/Distance Vector Multicast Routing Protocol (PIM/DVMRP) packets or to listen to CGMP self-join packets. By default, the switch snoops on PIM/DVMRP packets on all VLANs. To learn of multicast router ports through only CGMP self-join packets, use the **ip igmp snooping vlan *vlan\_id* mrouter learn cgmp** global configuration command. When this command is used, the router listens only to CGMP self-join packets and no other CGMP packets. To learn of multicast router ports through only PIM-DVMRP packets, use the **ip igmp snooping vlan *vlan\_id* mrouter learn pim-dvmrp** interface command.

## Joining a Multicast Group

When a host connected to the switch wants to join an IP multicast group, it sends an IGMP join message, specifying the IP multicast group it wants to join. When the switch receives this message, it adds the port to the IP multicast group port address entry in the forwarding table.

**Figure 4-32 Initial IGMP Join Message**



Refer to [Figure 4-32](#). Host 1 wants to join multicast group 224.1.2.3 and multicasts an unsolicited IGMP membership report (IGMP join message) to the group with the equivalent MAC destination address of 0100.5E01.0203. The switch recognizes IGMP packets and forwards them to the CPU. When the CPU receives the IGMP report multicast by Host 1, the CPU uses the information to set up a multicast forwarding table entry as shown in [Table 4-4](#) that includes the port numbers of Host 1 and the router.

**Table 4-4 IP Multicast Forwarding Table**

| Destination Address | Type of Packet | Ports |
|---------------------|----------------|-------|
| 0100.5e01.0203      | !IGMP          | 1, 2  |

Note that the architecture of the switch allows the CPU to distinguish IGMP information packets from other packets for the multicast group. The switch recognizes the IGMP packets through its filter engine. This prevents the CPU from becoming overloaded with multicast frames.

The entry in the multicast forwarding table tells the switching engine to send frames addressed to the 0100.5E01.0203 multicast MAC address that are not IGMP packets (!IGMP) to the router and to the host that has joined the group.

If another host (for example, Host 4) sends an IGMP join message for the same group (Figure 4-33), the CPU receives that message and adds the port number of Host 4 to the CAM table as shown in Table 4-5.

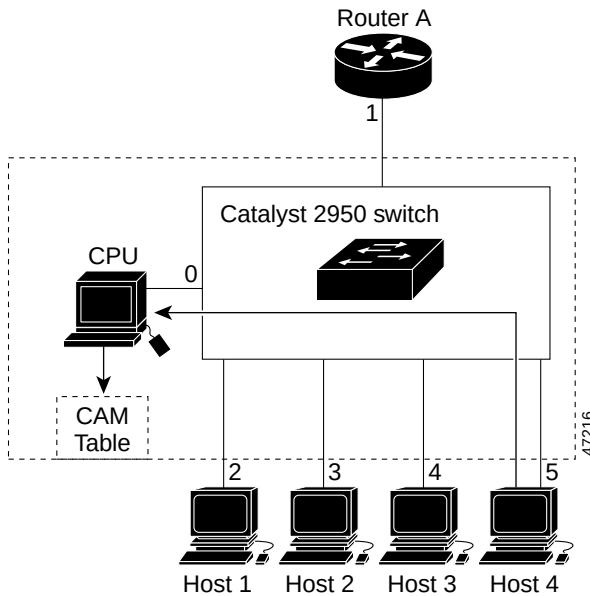
**Figure 4-33 Second Host Joining a Multicast Group**

**Table 4-5 Updated Multicast Forwarding Table**

| Destination Address | Type of Packet | Ports   |
|---------------------|----------------|---------|
| 0100.5e01.0203      | !IGMP          | 1, 2, 5 |

## Statically Configuring a Host to Join a Group

Ports normally join multicast groups through the IGMP report message, but you can also statically configure a host on an interface.

Select the **Multicast Group** tab on the IGMP snooping window (Figure 4-30) to view the current settings. Select the row you want to modify from the Multicast Groups window (Figure 4-34), and click **Modify** to change the settings. Use the Multicast Groups window (Figure 4-35) to add or remove ports from a multicast group.

Figure 4-34 Multicast Groups

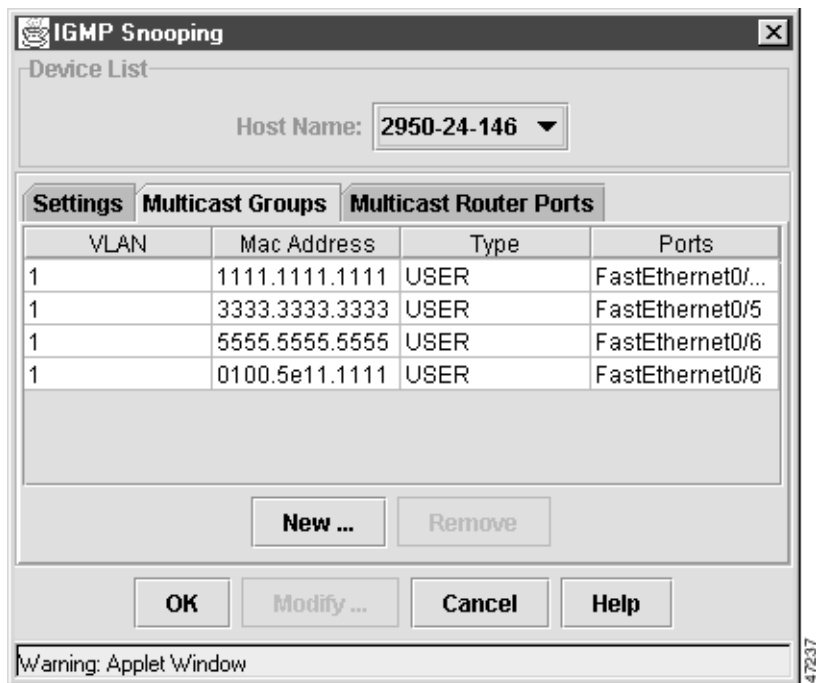
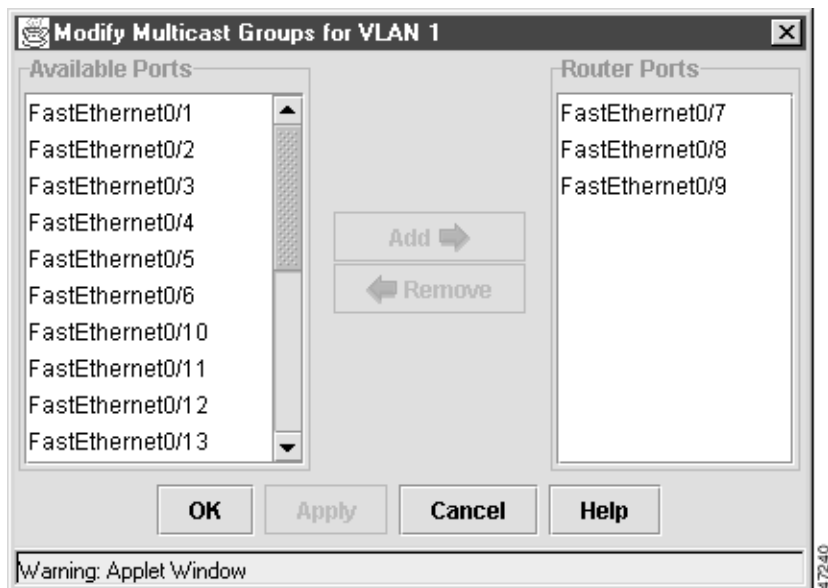


**Figure 4-35 Modify Multicast Groups**

## CLI: Statically Configuring a Interface to Join a Group

Beginning in privileged EXEC mode, follow these steps to add a port as a member of a multicast group:

|        | Command                                                                                                                        | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------|--------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>                                                                                                      | Enter global configuration mode                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Step 2 | <b>ip igmp snooping vlan <i>vlan_id</i></b><br><b>static <i>mac-address</i> interface</b><br><b><i>interface-num</i></b>       | Statically configure a port as a member of a multicast group: <ul style="list-style-type: none"><li>• <b>vlan_id</b> is the multicast group VLAN ID.</li><li>• <b>mac-address</b> is the group MAC address.</li><li>• <b>interface</b> is the member port.</li><li>• <b>FastEthernet <i>interface number</i></b> to specify a Fast Ethernet 802.3 interface.</li><li>• <b>Gigabit Ethernet <i>interface-number</i></b> to specify a Gigabit Ethernet 802.3z interface.</li></ul> |
| Step 3 | <b>end</b>                                                                                                                     | Return to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Step 4 | <b>show mac-address-table</b><br><b>multicast [<i>vlan vlan-id</i>] [<i>user</i>  </b><br><b>igmp-snooping] [<i>count</i>]</b> | Display MAC address table entries for a VLAN. <ul style="list-style-type: none"><li>• <b>vlan_id</b> (Optional) is the multicast group VLAN ID.</li><li>• <b>user</b> displays only the user-configured multicast entries.</li><li>• <b>igmp-snooping</b> displays entries learned via IGMP snooping.</li><li>• <b>count</b> displays only the total number of entries for the selected criteria, not the actual entries.</li></ul>                                              |
| Step 5 | <b>copy running-config</b><br><b>startup-config</b>                                                                            | (Optional) Save your configuration to the startup configuration.                                                                                                                                                                                                                                                                                                                                                                                                                 |

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## Leaving a Multicast Group

The router sends periodic IP multicast general queries, and the switch responds to these queries with one join response per MAC multicast group. As long as at least one host in the VLAN needs multicast traffic, the switch responds to the router queries, and the router continues forwarding the multicast traffic to the VLAN. The switch only forwards IP multicast group traffic to those hosts listed in the forwarding table for that IP multicast group.

When hosts need to leave a multicast group, they can either ignore the periodic general-query requests sent by the router, or they can send a leave message. When the switch receives a leave message from a host, it sends out a group-specific query to determine if any devices behind that interface are interested in traffic for the specific multicast group. If, after a number of queries, the router processor receives no reports from a VLAN, it removes the group for the VLAN from its IGMP cache.

## Configuring a Multicast Router Port

Select the **Multicast Router Port** tab on the IGMP snooping window ([Figure 4-30](#)) to view the current settings. Select the row that you want to modify from the Multicast Router Ports window ([Figure 4-36](#)), and click **Modify** to change the settings. Use the Multicast Router Ports window ([Figure 4-37](#)) to add or remove ports.



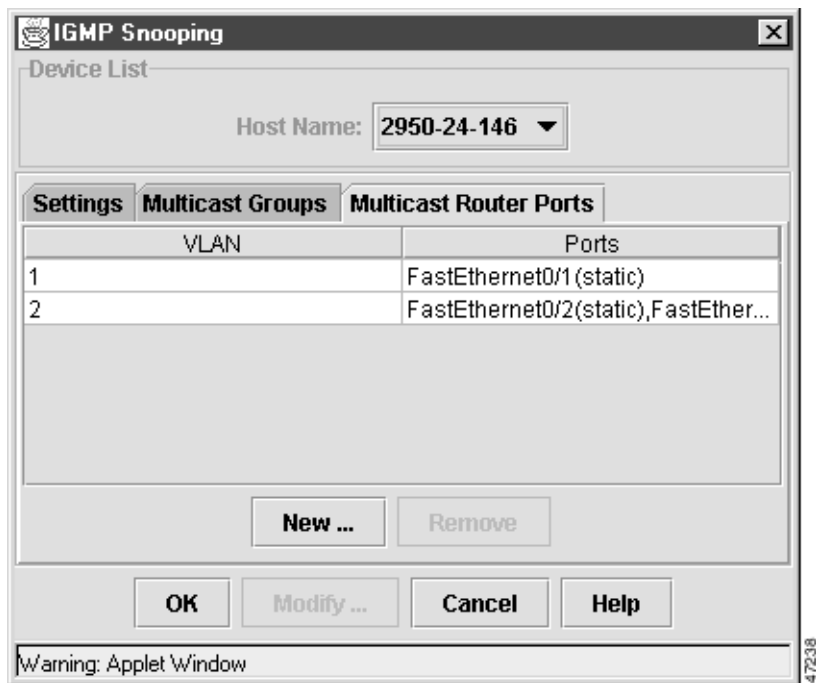
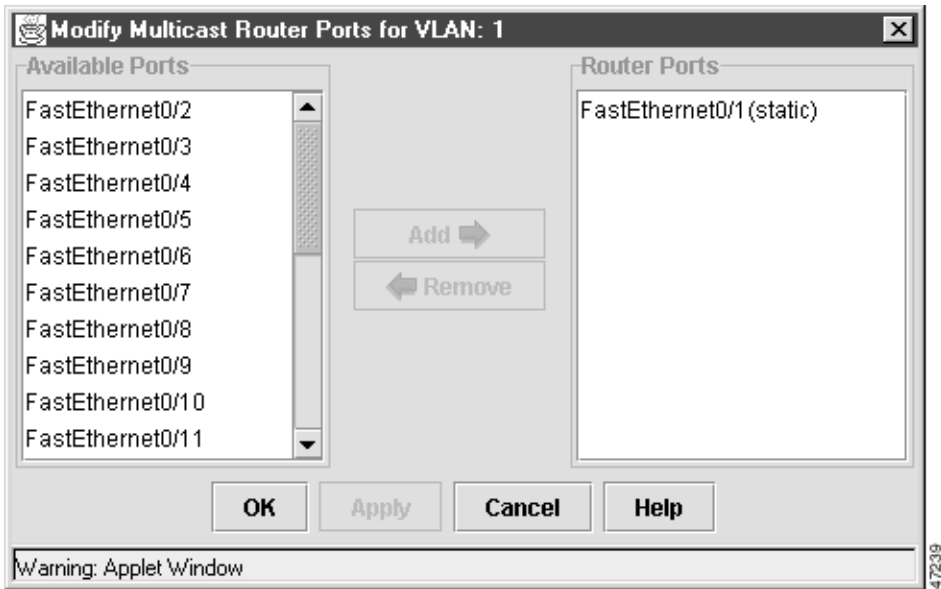
**Figure 4-36 Multicast Router Ports**

**Figure 4-37** *Modify Multicast Router Ports*

47239

## CLI: Configuring a Multicast Router Port

Beginning in privileged EXEC mode, follow these steps to enable a static connection to a multicast router:

|        | Command                                                                                                                    | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------|----------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>                                                                                                  | Enter global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Step 2 | <b>ip igmp snooping vlan <i>vlan_id</i></b><br><b>mrouter {<i>interface interface</i>}</b><br><b>{<i>learn method</i>}</b> | Specify the multicast router VLAN ID (1 to 1001).<br><br>Specify the interface to the multicast router as one of the following: <ul style="list-style-type: none"> <li>• <b>FastEthernet</b> <i>interface number</i> to specify a Fast Ethernet 802.3 interface (fa0/x, where x is the port number).</li> <li>• <b>GigabitEthernet</b> <i>interface-number</i> to specify a Gigabit Ethernet 802.3z interface (gi0/x, where x is the port number).</li> </ul><br>Specify the multicast router learning method: <ul style="list-style-type: none"> <li>• <b>cgmp</b> to specify listening for CGMP packets.</li> <li>• <b>pim-dvmrp</b> to specify snooping PIM-DVMRP packets</li> </ul> |
| Step 3 | <b>end</b>                                                                                                                 | Return to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Step 4 | <b>show ip igmp snooping [vlan <i>vlan_id</i>]</b>                                                                         | Verify that IGMP snooping is enabled on the VLAN interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Step 5 | <b>show ip igmp snooping mrouter [vlan <i>vlan_id</i>]</b>                                                                 | Display information on dynamically learned and manually configured multicast router interfaces.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Step 6 | <b>copy running-config startup-config</b>                                                                                  | (Optional) Save your configuration to the startup configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## Configuring the Spanning Tree Protocol

Spanning Tree Protocol (STP) provides path redundancy while preventing undesirable loops in the network. Only one active path can exist between any two stations. STP calculates the best loop-free path throughout the network.

### Supported STP Instances

You create an STP instance when you assign an interface to a VLAN. The STP instance is removed when the last interface is moved to another VLAN. You can configure switch and port parameters before an STP instance is created. These parameters are applied when the STP instance is created. You can change all VLANs on a switch by using the **show spanning-tree [vlan *stp-list*]** privileged EXEC command when you enter STP commands through the CLI. For more information, refer to the *Catalyst 2950 Desktop Switch Command Reference*.

Catalyst 2950 switches support only 64 VLANs. For more information about VLANs, see [Chapter 5, “Creating and Maintaining VLANs.”](#)

Each VLAN is a separate STP instance. If you have already used up all available STP instances on a switch, adding another VLAN anywhere in the VLAN Trunk Protocol (VTP) domain creates a VLAN that is not running STP on that switch. For example, if 64 VLANs are defined in the VTP domain, you can enable STP on those 64 VLANs. The remaining VLANs must operate with STP disabled.

You can disable STP on one of the VLANs where it is running and then enable it on the VLAN where you want it to run. Use the **no spanning-tree vlan *vlan-id*** global configuration command to disable STP on a specific VLAN, and use the **spanning-tree vlan *vlan-id*** global configuration command to enable STP on the desired VLAN.

**Caution**

Switches that are not running spanning tree still forward BPDUs that they receive so that the other switches on the VLAN that have a running STP instance can break loops. Therefore, spanning tree must be running on enough switches so that it can break all the loops in the network. For example, at least one switch on each loop in the VLAN must be running spanning tree. It is not absolutely necessary to run spanning tree on all switches in the VLAN; however, if you are running STP only on a minimal set of switches, an incautious change to the network that introduces another loop into the VLAN can result in a broadcast storm.

**Note**

If you have the default allowed list on the trunk ports of that switch, the new VLAN is carried on all trunk ports. Depending on the topology of the network, this could create a loop in the new VLAN that will not be broken, particularly if there are several adjacent switches that all have run out of STP instances. You can prevent this by setting allowed lists on the trunk ports of switches that have used up their allocation of STP instances. Setting up allowed lists is not necessary in many cases and adding another VLAN to the network would become more labor-intensive.

Use the Spanning Tree Protocol (STP) window ([Figure 4-38](#)) to change parameters for STP, an industry standard for avoiding loops in switched networks. Each VLAN supports its own instance of STP.

Spanning Tree Protocol (STP) provides path redundancy while preventing undesirable loops in the network. Only one active path can exist between any two stations. STP calculates the best loop-free path throughout the network.

You can use this window to perform the following tasks:

- Disable STP for a switch or group of switches.
- Change STP parameters for per VLAN (STP implementation, switch priority, Bridge Protocol Data Unit (BPDU) message interval, hello BPDU interval, and the forwarding time).
- Change STP port parameters per VLAN (Port Fast feature, root cost, path cost, port priority).

- Display the STP parameters and port parameters for the switch currently acting as the STP root switch.

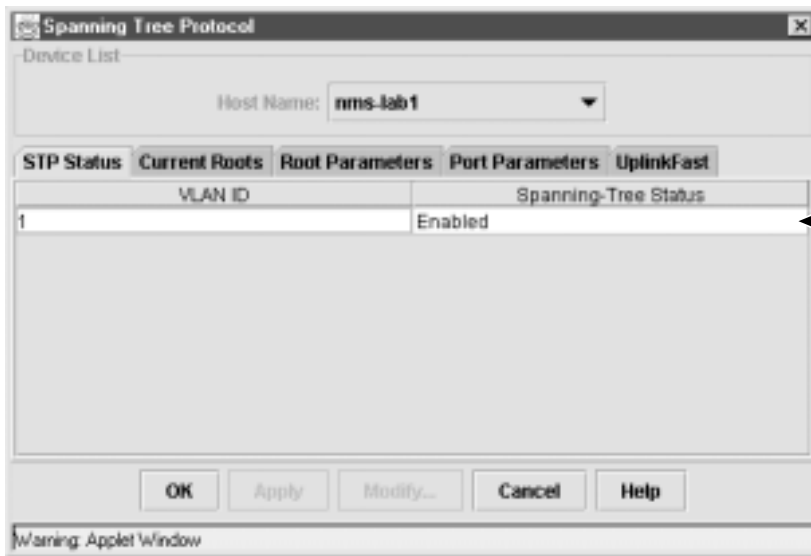
**Note**

VLANs are identified with a number between 1 and 1001. Regardless of the switch model, only 64 possible instances of STP are supported.

To display this window, select **Device > Spanning Tree Protocol** from the menu bar to display STP information for the command switch, or right-click a switch, and select **Device > Spanning Tree Protocol** from the pop-up menu to display the STP information defined for that switch. You can also click the STP icon on the toolbar.

The STP rootguard option is described in the [“CLI: Configuring STP Root Guard” section on page 4-98](#).

**Figure 4-38 Spanning Tree Protocol —Status**



Each VLAN is a separate instance of STP.

29665

## Using STP to Support Redundant Connectivity

You can create a redundant backbone with STP by connecting two of the switch ports to another device or to two different devices. STP automatically disables one port but enables it if the other port is lost. If one link is high-speed and the other low-speed, the low-speed link is always disabled. If the speed of the two links is the same, the port priority and port ID are added together, and STP disables the link with the lowest value.

You can also create redundant links between switches by using EtherChannel port groups. For more information on creating port groups, see the [“Creating EtherChannel Port Groups” section on page 4-11](#).

## Accelerating Aging to Retain Connectivity

The default for aging dynamic addresses is 5 minutes. However, a reconfiguration of the spanning tree can cause many station locations to change. Because these stations could be unreachable for 5 minutes or more during a reconfiguration, the address-aging time is accelerated so that station addresses can be dropped from the address table and then relearned. The accelerated aging is the same as the forward-delay parameter value when STP reconfigures.

Because each VLAN is a separate instance of STP, the switch accelerates aging on a per-VLAN basis. A reconfiguration of STP on one VLAN can cause the dynamic addresses learned on that VLAN to be subject to accelerated aging. Dynamic addresses on other VLANs can be unaffected and remain subject to the aging interval entered for the switch.

## Disabling STP Protocol

STP is enabled by default. Disable STP only if you are sure there are no loops in the network topology.

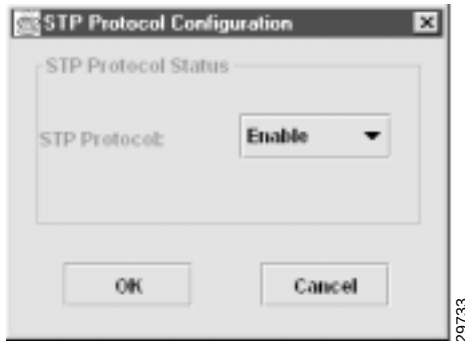


### Caution

---

When STP is disabled and loops are present in the topology, excessive traffic and indefinite packet duplication can drastically reduce network performance.

---

**Figure 4-39 STP Pop-up**

## CLI: Disabling STP

Beginning in privileged EXEC mode, follow these steps to disable STP:

|        | Command                                      | Purpose                          |
|--------|----------------------------------------------|----------------------------------|
| Step 1 | <b>configure terminal</b>                    | Enter global configuration mode. |
| Step 2 | <b>no spanning-tree vlan <i>stp-list</i></b> | Disable STP on a VLAN.           |
| Step 3 | <b>end</b>                                   | Return to privileged EXEC mode.  |
| Step 4 | <b>show spanning-tree</b>                    | Verify your entry.               |

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## Configuring Redundant Links By Using STP UplinkFast

Switches in hierarchical networks can be grouped into backbone switches, distribution switches, and access switches. [Figure 4-40](#) shows a complex network where distribution switches and access switches each have at least one redundant link that STP blocks to prevent loops.

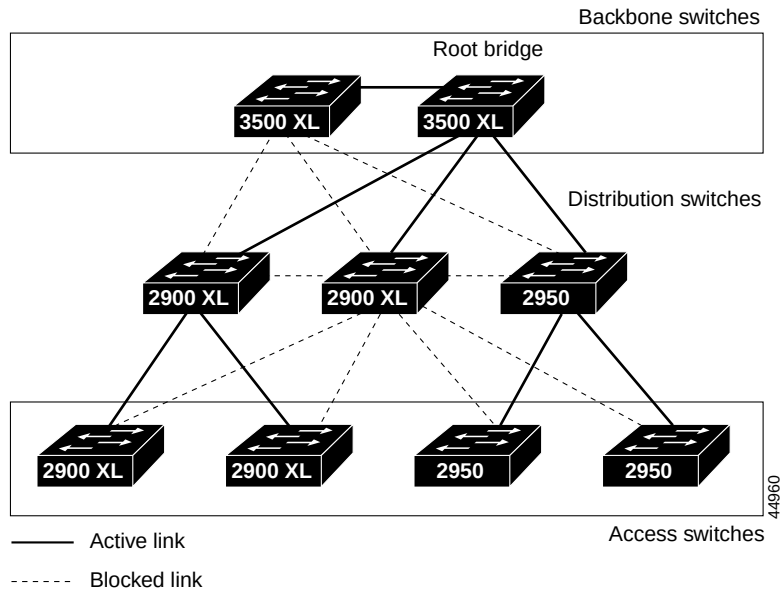


If a switch loses connectivity, the switch begins using the alternate paths as soon as STP selects a new root port. When STP reconfigures the new root port, other ports flood the network with multicast packets, one for each address that was learned on the port. You can limit these bursts of multicast traffic by reducing the max-update-rate parameter (the default for this parameter is 150 packets per second). However, if you enter zero, station-learning frames are not generated, so the STP topology converges more slowly after a loss of connectivity.

STP UplinkFast is an enhancement that accelerates the choice of a new root port when a link or switch fails or when STP reconfigures itself. The root port transitions to the forwarding state immediately without going through the listening and learning states, as it would with normal STP procedures. UplinkFast is most useful in edge or access switches and might not be appropriate for backbone devices.

You can change STP parameters by using the UplinkFast tab of the Spanning Tree Protocol window or by using the CLI. The [“Configuring the Spanning Tree Protocol” section on page 4-80](#) describes the use of the Spanning Tree Protocol window.

To display this window, select **Device > Spanning-Tree Protocol** from the menu bar. Then click the **UplinkFast** tab.

**Figure 4-40 Switches in a Hierarchical Network**

## CLI: Enabling STP UplinkFast

When you enable UplinkFast, it is enabled for the entire switch and cannot be enabled for individual VLANs.

Beginning in privileged EXEC mode, follow these steps to configure UplinkFast:

|        | Command                                                                          | Purpose                                                                                                                                                                                                                                                         |
|--------|----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>                                                        | Enter global configuration mode.                                                                                                                                                                                                                                |
| Step 2 | <b>spanning-tree uplinkfast</b><br><b>max-update-rate</b> <i>pkts-per-second</i> | Enable UplinkFast on the switch.<br><br>The range is from 0 to 1000 packets per second; The default is 150.<br><br>If you set the rate to 0, station-learning frames are not generated, so the STP topology converges more slowly after a loss of connectivity. |
| Step 3 | <b>exit</b>                                                                      | Return to privileged EXEC mode.                                                                                                                                                                                                                                 |
| Step 4 | <b>show spanning-tree</b>                                                        | Verify your entries.                                                                                                                                                                                                                                            |

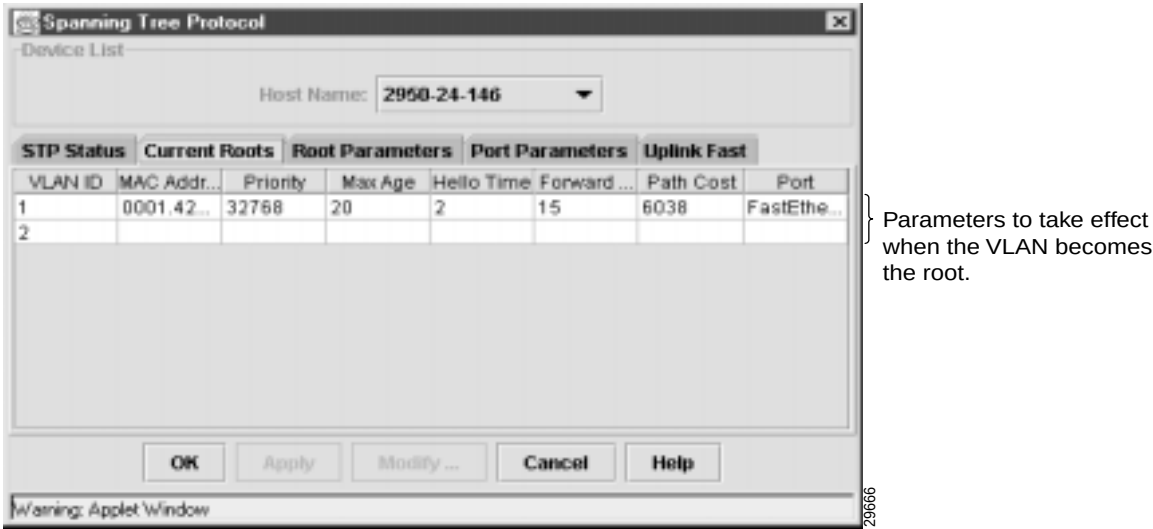
When UplinkFast is enabled, the bridge priority of all VLANs is set to 49152, and the path cost of all ports and VLAN trunks is increased by 3000. This change reduces the chance that the switch will become the root port. When UplinkFast is disabled, the bridge priorities of all VLANs and path costs of all ports are set to default values.

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## Changing STP Parameters for a VLAN

To change STP parameters for a VLAN, select **Device > Spanning Tree Protocol** from the menu bar, select the VLAN ID of the STP instance to change, and click **Root Parameters**.

Figure 4-41 Spanning Tree Protocol Current Root Tab



In [Figure 4-41](#), the parameters under the heading Current Spanning-Tree Root are read-only. The MAC Address field shows the MAC address of the switch currently acting as the root for each VLAN; the remaining parameters show the other STP settings for the root switch for each VLAN. The root switch is the switch with the highest priority and transmits topology frames to other switches in the spanning tree.

In the Spanning Tree Protocol window ([Figure 4-42](#)), you can change the root parameters for the VLANs on a selected switch. The following fields ([Figure 4-42](#)) define how your switch responds when STP reconfigures itself.

- Protocol

Implementation of STP to use.  
Select one of the menu bar items: IBM, or IEEE. The default is IEEE.
- Priority

Value used to identify the root switch. The switch with the **lowest value** has the highest priority and is selected as the root.  
Enter a number from 0 to 65535.

|               |                                                                                                                                                                                                                                                                                                                  |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Max age       | <p>Number of seconds a switch waits without receiving STP configuration messages before attempting a reconfiguration. This parameter takes effect when a switch is operating as the root switch. Switches not acting as the root use the root-switch Max age parameter.</p> <p>Enter a number from 6 to 200.</p> |
| Hello Time    | <p>Number of seconds between the transmission of hello messages, which indicate that the switch is active. Switches not acting as a root switch use the root-switch Hello-time value.</p> <p>Enter a number from 1 to 10.</p>                                                                                    |
| Forward Delay | <p>Number of seconds a port waits before changing from its STP learning and listening states to the forwarding state. This wait is necessary so that other switches on the network ensure no loop is formed before they allow the port to forward packets.</p> <p>Enter a number from 4 to 200.</p>              |

Figure 4-42 Spanning Tree Protocol Root Parameters Tab

**Spanning Tree Protocol**

Device List

Host Name: 2950-24-146

**STP Status** **Current Roots** **Root Parameters** **Port Parameters** **Uplink Fast**

| VLAN ID | Protocol | Priority | Max Age | Hello Time | Forward Delay |
|---------|----------|----------|---------|------------|---------------|
| 1       | IEEE     | 49152    | 20      | 2          | 15            |
| 2       | IEEE     | 32768    | 20      | 2          | 15            |

OK Apply Modify ... Cancel Help

Warning: Applet Window

29734

## CLI: Changing the STP Implementation

Beginning in privileged EXEC mode, follow these steps to change the STP implementation. The *stp-list* is the list of VLANs to which the STP command applies.

|        | Command                                                               | Purpose                                                                 |
|--------|-----------------------------------------------------------------------|-------------------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>                                             | Enter global configuration mode.                                        |
| Step 2 | <b>spanning-tree [vlan <i>stp-list</i>]<br/>protocol {ieee   ibm}</b> | Specify the STP implementation to be used for a spanning-tree instance. |
| Step 3 | <b>end</b>                                                            | Return to privileged EXEC mode.                                         |
| Step 4 | <b>show spanning-tree</b>                                             | Verify your entry.                                                      |

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## CLI: Changing the Switch Priority

Beginning in privileged EXEC mode, follow these steps to change the switch priority and affect which switch is the root switch. The *stp-list* is the list of VLANs to which the STP command applies.

|        | Command                                                                         | Purpose                                                                                                                                                                                            |
|--------|---------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>                                                       | Enter global configuration mode.                                                                                                                                                                   |
| Step 2 | <b>spanning-tree [vlan <i>stp-list</i>]<br/>priority <i>bridge-priority</i></b> | Configure the switch priority for the specified spanning-tree instance.<br><br>Enter a number from 0 to 65535; the lower the number, the more likely the switch will be chosen as the root switch. |
| Step 3 | <b>end</b>                                                                      | Return to privileged EXEC mode.                                                                                                                                                                    |
| Step 4 | <b>show spanning-tree</b>                                                       | Verify your entry.                                                                                                                                                                                 |

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## CLI: Changing the BPDU Message Interval

Beginning in privileged EXEC mode, follow these steps to change the BPDU message interval (max age time). The *stp-list* is the list of VLANs to which the STP command applies.

|        | Command                                                                | Purpose                                                                                                                                                                                                                                                               |
|--------|------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>                                              | Enter global configuration mode.                                                                                                                                                                                                                                      |
| Step 2 | <b>spanning-tree [vlan <i>stp-list</i>]<br/>max-age <i>seconds</i></b> | Specify the interval between messages the spanning tree receives from the root switch.<br><br>The maximum age is the number of seconds a switch waits without receiving STP configuration messages before attempting a reconfiguration. Enter a number from 6 to 200. |
| Step 3 | <b>end</b>                                                             | Return to privileged EXEC mode.                                                                                                                                                                                                                                       |
| Step 4 | <b>show spanning-tree</b>                                              | Verify your entry.                                                                                                                                                                                                                                                    |

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## CLI: Changing the Hello BPDU Interval

Beginning in privileged EXEC mode, follow these steps to change the hello BPDU interval (hello time). The *stp-list* is the list of VLANs to which the STP command applies.

|        | Command                                                                   | Purpose                                                                                                                          |
|--------|---------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>                                                 | Enter global configuration mode.                                                                                                 |
| Step 2 | <b>spanning-tree [vlan <i>stp-list</i>]<br/>hello-time <i>seconds</i></b> | Specify the interval between hello BPDUs.<br><br>Hello messages indicate that the switch is active. Enter a number from 1 to 10. |
| Step 3 | <b>end</b>                                                                | Return to privileged EXEC mode.                                                                                                  |
| Step 4 | <b>show spanning-tree</b>                                                 | Verify your entry.                                                                                                               |



The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## CLI: Changing the Forwarding Delay Time

Beginning in privileged EXEC mode, follow these steps to change the forwarding delay time. The *stp-list* is the list of VLANs to which the STP command applies.

|        | Command                                                                     | Purpose                                                                                                                                                                                                                                                |
|--------|-----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>                                                   | Enter global configuration mode.                                                                                                                                                                                                                       |
| Step 2 | <b>spanning-tree [vlan <i>stp-list</i>]<br/>forward-time <i>seconds</i></b> | Specify the forwarding time for the specified spanning-tree instance.<br><br>The forward delay is the number of seconds a port waits before changing from its STP learning and listening states to the forwarding state. Enter a number from 4 to 200. |
| Step 3 | <b>end</b>                                                                  | Return to privileged EXEC mode.                                                                                                                                                                                                                        |
| Step 4 | <b>show spanning-tree</b>                                                   | Verify your entry.                                                                                                                                                                                                                                     |

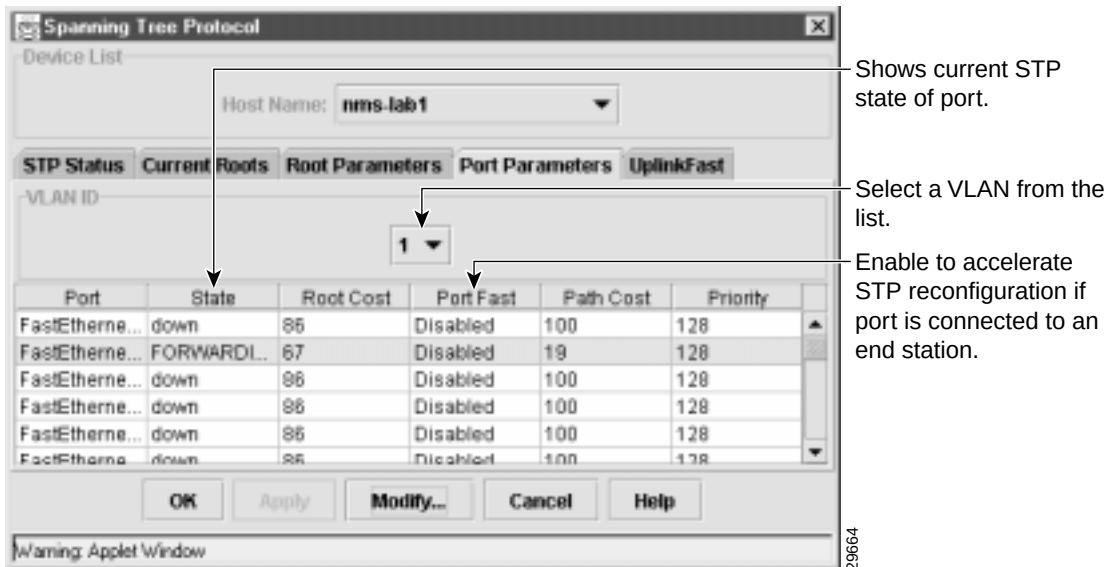
The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## Changing STP Port Parameters

The ports listed on this window ([Figure 4-43](#)) belong to the VLAN selected in the VLAN ID list above the table of parameters. To change STP port options, select **Device > Spanning Tree Protocol** from the menu bar, select the VLAN ID, and click **Modify STP Parameters**.

Use the following fields ([Figure 4-43](#)) to check the status of ports that are not forwarding due to STP:

|            |                                                                                                                                                                                                                |
|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Port       | The interface and port number. FastEthernet0/1 refers to port 1x.                                                                                                                                              |
| State      | The current state of the port. A port can be in one of the following states:                                                                                                                                   |
| Listening  | Port is not participating in the frame-forwarding process, but is progressing towards a forwarding state. The port is not learning addresses.                                                                  |
| Learning   | Port is not forwarding frames but is learning addresses.                                                                                                                                                       |
| Forwarding | Port is forwarding frames and learning addresses.                                                                                                                                                              |
| Disabled   | Port has been removed from STP operation.                                                                                                                                                                      |
| Down       | Port has no physical link.                                                                                                                                                                                     |
| Broken     | One end of the link is configured as an access port and the other end is configured as an 802.1Q trunk port, or both ends of the link are configured as 802.1Q trunk ports but have different native VLAN IDs. |

**Figure 4-43 Spanning Tree Protocol Port Parameters Tab**

## Enabling the Port Fast Feature

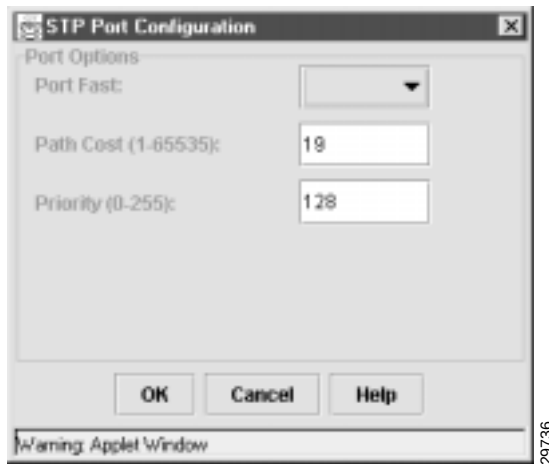
The Port Fast feature brings a port directly from a blocking state into a forwarding state. This feature is useful when a connected server or workstation times out because its port is going through the normal cycle of STP status changes. The only time a port with Port Fast enabled goes through the normal cycle of STP status changes is when the switch is restarted.

To enable the Port Fast feature on the Port Configuration pop-up (Figure 4-44), select a row in the Port Parameters tab, and click **Modify**.



### Caution

Enabling this feature on a port connected to a switch or hub could prevent STP from detecting and disabling loops in your network, and this could cause broadcast storms and address-learning problems.

**Figure 4-44 STP Port Configuration Pop-up**

You can modify the following parameters and enable the Port Fast feature by selecting a row on the Port Parameters tab and clicking **Modify**.

- |           |                                                                                                                                                                                                                                                                                                               |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Port Fast | Enable to bring the port more quickly to an STP forwarding state.                                                                                                                                                                                                                                             |
| Path Cost | <p>A lower path cost represents higher-speed transmission. This can affect which port remains enabled in the event of a loop.</p> <p>Enter a number from 1 to 65535. The default is 100 for 10 Mbps, 19 for 100 Mbps, 4 for 1 Gbps, 2 for 10 Gbps, and 1 for interfaces with speeds greater than 10 Gbps.</p> |
| Priority  | Number used to set the priority for a port. A higher number has higher priority. Enter a number from 0 to 65535.                                                                                                                                                                                              |

## CLI: Enabling STP Port Fast

Enabling this feature on a port connected to a switch or hub could prevent STP from detecting and disabling loops in your network. Beginning in privileged EXEC mode, follow these steps to enable the Port Fast feature:

|        | Command                           | Purpose                                                                  |
|--------|-----------------------------------|--------------------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>         | Enter global configuration mode.                                         |
| Step 2 | <b>interface</b> <i>interface</i> | Enter interface configuration mode, and enter the port to be configured. |
| Step 3 | <b>spanning-tree portfast</b>     | Enable the Port Fast feature for the port.                               |
| Step 4 | <b>end</b>                        | Return to privileged EXEC mode.                                          |
| Step 5 | <b>show running-config</b>        | Verify your entry.                                                       |

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## CLI: Changing the Path Cost

Beginning in privileged EXEC mode, follow these steps to change the path cost for STP calculations. The STP command applies to the *stp-list*.

|        | Command                                                         | Purpose                                                                                              |
|--------|-----------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>                                       | Enter global configuration mode.                                                                     |
| Step 2 | <b>interface</b> <i>interface</i>                               | Enter interface configuration mode, and enter the port to be configured.                             |
| Step 3 | <b>spanning-tree [vlan <i>stp-list</i>] cost</b><br><i>cost</i> | Configure the path cost for the specified spanning-tree instance.<br>Enter a number from 1 to 65535. |
| Step 4 | <b>end</b>                                                      | Return to privileged EXEC mode.                                                                      |
| Step 5 | <b>show running-config</b>                                      | Verify your entry.                                                                                   |

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## CLI: Changing the Port Priority

Beginning in privileged EXEC mode, follow these steps to change the port priority, which is used when two switches tie for position as the root switch. The *stp-list* is the list of VLANs to which the STP command applies.

|        | Command                                                                                   | Purpose                                                                                                                                          |
|--------|-------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>                                                                 | Enter global configuration mode.                                                                                                                 |
| Step 2 | <b>interface</b> <i>interface</i>                                                         | Enter interface configuration mode, and enter the port to be configured.                                                                         |
| Step 3 | <b>spanning-tree</b> [vlan <i>stp-list</i> ]<br><b>port-priority</b> <i>port-priority</i> | Configure the port priority for a specified instance of STP.<br><br>Enter a number from 0 to 255. The lower the number, the higher the priority. |
| Step 4 | <b>end</b>                                                                                | Return to privileged EXEC mode.                                                                                                                  |
| Step 5 | <b>show running-config</b>                                                                | Verify your entry.                                                                                                                               |

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

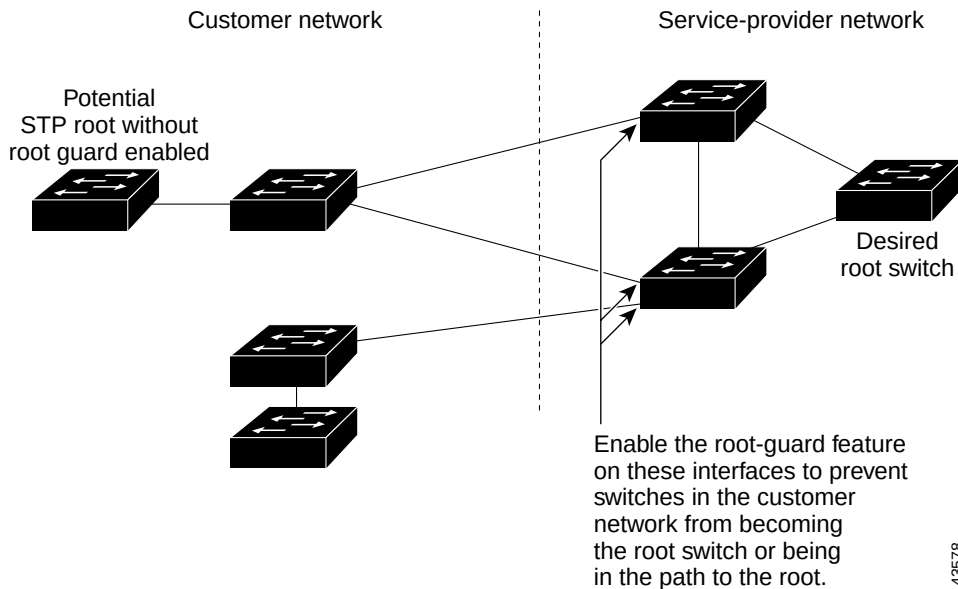
## CLI: Configuring STP Root Guard

The Layer 2 network of a service provider (SP) can include many connections to switches that are not owned by the SP. In such a topology, STP can reconfigure itself and select a *customer switch* as the STP root switch, as shown in [Figure 4-45](#). You can avoid this possibility by configuring the root guard parameter on ports that connect to switches outside of your network. If a switch outside the network becomes the root switch, the port is blocked, and STP selects a new root switch.



### Caution

Misuse of this command can cause a loss of connectivity.

**Figure 4-45 STP in a Service Provider Network**

Root guard enabled on a port applies to all the VLANs that the port belongs to. Each VLAN has its own instance of STP.

Beginning in privileged EXEC mode, follow these steps to set root guard on a port:

|        | Command                           | Purpose                                                                  |
|--------|-----------------------------------|--------------------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>         | Enter global configuration mode.                                         |
| Step 2 | <b>interface</b> <i>interface</i> | Enter interface configuration mode, and enter the port to be configured. |
| Step 3 | <b>spanning-tree rootguard</b>    | Enable root guard on the port.                                           |
| Step 4 | <b>end</b>                        | Return to privileged EXEC mode.                                          |
| Step 5 | <b>show running-config</b>        | Verify that the port is configured for root guard.                       |

Use the **no** version of the **spanning-tree rootguard** command to disable the root guard feature.

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## CLI: Configuring UniDirectional Link Detection

UniDirectional Link Detection (UDLD) is a Layer 2 protocol that detects and shuts down unidirectional links. You can configure UDLD on the entire switch or on an individual port.

Beginning in privileged EXEC mode, follow these steps to configure UDLD on a switch:

|        | Command                    | Purpose                                                   |
|--------|----------------------------|-----------------------------------------------------------|
| Step 1 | <b>configure terminal</b>  | Enter global configuration mode.                          |
| Step 2 | <b>udld enable</b>         | Enable UDLD.                                              |
| Step 3 | <b>end</b>                 | Return to privileged EXEC mode.                           |
| Step 4 | <b>show running-config</b> | Verify the entry by displaying the running configuration. |

Use the **udld reset** command to reset any port that has been shut down by UDLD.

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## Configuring Protected Ports

Some applications require that no traffic be forwarded by the Layer 2 protocol between ports on the same switch. In such an environment, there is no exchange of unicast, broadcast, or multicast traffic between ports on the switch, and traffic between ports on the same switch is forwarded through a Layer 3 device such as a router.

To meet this requirement, you can configure Catalyst 2950, 2900 XL, and 3500 XL ports as protected ports. Protected ports do not forward any traffic to protected ports on the same switch. This means that all traffic passing between



protected ports—unicast, broadcast, and multicast—must be forwarded through a Layer 3 device. Protected ports can forward any type of traffic to nonprotected ports, and they forward as usual to all ports on other switches.

**Note**

There could be times when unknown unicast traffic from a nonprotected port is flooded to a protected port because a MAC address has timed out or has not been learned by the switch.

## CLI: Configuring Protected Ports

Beginning in privileged EXEC mode, follow these steps to define a port as a protected port:

|        | Command                           | Purpose                                                                  |
|--------|-----------------------------------|--------------------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>         | Enter global configuration mode.                                         |
| Step 2 | <b>interface</b> <i>interface</i> | Enter interface configuration mode, and enter the port to be configured. |
| Step 3 | <b>port protected</b>             | Enable protected port on the port.                                       |
| Step 4 | <b>end</b>                        | Return to privileged EXEC mode.                                          |
| Step 5 | <b>show port protected</b>        | Verify that the port has protected port enabled.                         |

Use the **no** version of the **port protected** command to disable protected port.

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## Configuring TACACS+

The Terminal Access Controller Access Control System Plus (TACACS+) provides the means to manage network security (authentication, authorization, and accounting [AAA]) from a server. This section describes how TACACS+

works and how you can configure it. For complete syntax and usage information for the commands described in this chapter, refer to the *Cisco IOS Release 12.0 Security Command Reference*.

You can only configure this feature by using the CLI; you cannot configure it through the Cluster Management Suite.

## Understanding TACACS+

In large enterprise networks, the task of administering passwords on each device can be simplified by centralizing user authentication on a server. TACACS+ is an access-control protocol that allows a switch to authenticate all login attempts through a central server. The network administrator configures the switch with the address of the TACACS+ server, and the switch and the server exchange messages to authenticate each user before allowing access to the management console.

TACACS+ consists of three services: authentication, authorization, and accounting. Authentication determines who the user is and whether or not the user is allowed access to the switch. Authorization is the action of determining what the user is allowed to do on the system. Accounting is the action of collecting data related to resource usage.

## CLI Procedures for Configuring TACACS+

The TACACS+ feature is disabled by default. However, you can enable and configure it by using the CLI. You can access the CLI through the console port or through Telnet. To prevent a lapse in security, you cannot configure TACACS+ through a network-management application. When enabled, TACACS+ can authenticate users accessing the switch through the CLI.



### Note

---

Although the TACACS+ configuration is performed through the CLI, the TACACS+ server authenticates HTTP connections that have been configured with a privilege level of 15.

---

## CLI: Configuring the TACACS+ Server Host

Use the **tacacs-server host** command to specify the names of the IP host or hosts maintaining an AAA/TACACS+ server. On TACACS+ servers, you can configure the following additional options:

- Number of seconds that the switch attempts to contact the server before it times out.
- Encryption key to encrypt and decrypt all traffic between the router and the daemon.
- Number of attempts that a user can make when entering a command that is being authenticated by TACACS+.

Beginning in privileged EXEC mode, follow these steps to configure the TACACS+ server:

|        | Command                                                                                              | Purpose                                                                                                                                                                                                                                                 |
|--------|------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>tacacs-server host</b> <i>name</i> [ <b>timeout</b> <i>integer</i> ] [ <b>key</b> <i>string</i> ] | Define a TACACS+ host.<br><br>Entering the <b>timeout</b> and <b>key</b> parameters with this command overrides the global values that you can enter with the <b>tacacs-server timeout</b> (Step 3) and the <b>tacacs-server key</b> commands (Step 5). |
| Step 2 | <b>tacacs-server retransmit</b> <i>retries</i>                                                       | Enter the number of times the server searches the list of TACACS+ servers before stopping.<br><br>The default is two.                                                                                                                                   |
| Step 3 | <b>tacacs-server timeout</b> <i>seconds</i>                                                          | Set the interval that the server waits for a TACACS+ server host to reply.<br><br>The default is 5 seconds.                                                                                                                                             |
| Step 4 | <b>tacacs-server attempts</b> <i>count</i>                                                           | Set the number of login attempts that can be made on the line.                                                                                                                                                                                          |

|        | Command                             | Purpose                                                                                                                                                                  |
|--------|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5 | <b>tacacs-server</b> <i>key key</i> | Define a set of encryption keys for all of TACACS+ and communication between the access server and the TACACS daemon.<br><br>Repeat the command for each encryption key. |
| Step 6 | <b>exit</b>                         | Return to privileged EXEC mode.                                                                                                                                          |
| Step 7 | <b>show tacacs</b>                  | Verify your entries.                                                                                                                                                     |

The “[Finding More Information About IOS Commands](#)” section on page 4-1 contains the path to the complete IOS documentation.

## CLI: Configuring Login Authentication

Beginning in privileged EXEC mode, follow these steps to configure login authentication by using AAA/TACACS+:

|        | Command                                                                                        | Purpose                                                                                                    |
|--------|------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>                                                                      | Enter global configuration mode.                                                                           |
| Step 2 | <b>aaa new-model</b>                                                                           | Enable AAA/TACACS+.                                                                                        |
| Step 3 | <b>aaa authentication login</b><br><b>{default   list-name} method1</b><br><b>[method2...]</b> | Enable authentication at login, and create one or more lists of authentication methods.                    |
| Step 4 | <b>line [aux   console   tty   vty]</b><br><b>line-number [ending-line-number]</b>             | Enter line configuration mode, and configure the lines to which you want to apply the authentication list. |
| Step 5 | <b>login authentication {default   list-name}</b>                                              | Apply the authentication list to a line or set of lines.                                                   |
| Step 6 | <b>exit</b>                                                                                    | Return to privileged EXEC mode.                                                                            |
| Step 7 | <b>show running-config</b>                                                                     | Verify your entries.                                                                                       |

The variable *list-name* is any character string used to name the list you are creating. The *method* variable refers to the actual methods the authentication algorithm tries, in the sequence entered. You can choose one of the following methods:

- line** Uses the line password for authentication. You must define a line password before you can use this authentication method. Use the **password** *password* line configuration mode command.
- local** Uses the local username database for authentication. You must enter username information into the database. Use the **username** *password* global configuration command.
- tacacs+** Uses TACACS+ authentication. You must configure the TACACS+ server before you can use this authentication method. For more information, see the [“CLI: Configuring the TACACS+ Server Host” section on page 4-103](#).

To create a default list that is used if **no list** is specified in the **login authentication** command, use the **default** keyword followed by the methods you want used in default situations.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication succeed even if all methods return an error, specify **none** as the final method in the command line.

The [“Finding More Information About IOS Commands” section on page 4-1](#) contains the path to the complete IOS documentation.

## CLI: Specifying TACACS+ Authorization for EXEC Access and Network Services

You can use the **aaa authorization** command with the **tacacs+** keyword to set parameters that restrict a user's network access to Cisco IOS privilege mode (EXEC access) and to network services such as Serial Line Internet Protocol (SLIP), Point-to-Point Protocol (PPP) with Network Control Protocols (NCPs), and AppleTalk Remote Access (ARA).

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

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

**Note**

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

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

|        | Command                                  | Purpose                                                                                                                                                                                                             |
|--------|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>                | Enter global configuration mode.                                                                                                                                                                                    |
| Step 2 | <b>aaa authorization network tacacs+</b> | Configure the switch for user TACACS+ authorization for all network-related service requests, including SLIP, PPP NCPs, and ARA protocols.                                                                          |
| Step 3 | <b>aaa authorization exec tacacs+</b>    | Configure the switch for user TACACS+ authorization to determine if the user is allowed EXEC access.<br><br>The <b>exec</b> keyword might return user profile information (such as <b>autocommand</b> information). |
| Step 4 | <b>exit</b>                              | Return to privileged EXEC mode.                                                                                                                                                                                     |

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## CLI: Starting TACACS+ Accounting

You use the **aaa accounting** command with the **tacacs+** keyword to turn on TACACS+ accounting for each Cisco IOS privilege level and for network services.

Beginning in privileged EXEC mode, follow these steps to enable TACACS+ accounting:

|        | Command                                          | Purpose                                                                                                                              |
|--------|--------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>                        | Enter global configuration mode.                                                                                                     |
| Step 2 | <b>aaa accounting exec start-stop tacacs+</b>    | Enable TACACS+ accounting to send a start-record accounting notice at the beginning of an EXEC process and a stop-record at the end. |
| Step 3 | <b>aaa accounting network start-stop tacacs+</b> | Enable TACACS+ accounting for all network-related service requests, including SLIP, PPP, and PPP NCPs.                               |
| Step 4 | <b>exit</b>                                      | Return to privileged EXEC mode.                                                                                                      |

**Note**

These commands are documented in the “Accounting and Billing Commands” chapter of the *Cisco IOS Release 12.0 Security Command Reference*.

## CLI: Configuring a Switch for Local AAA

You can configure AAA to operate without a server by setting the switch to implement AAA in local mode. Authentication and authorization are then handled by the switch. No accounting is available in this configuration.

Beginning in privileged EXEC mode, follow these steps to configure the switch for local AAA:

|        | Command                                       | Purpose                                          |
|--------|-----------------------------------------------|--------------------------------------------------|
| Step 1 | <b>configure terminal</b>                     | Enter global configuration mode.                 |
| Step 2 | <b>aaa new-model</b>                          | Enable AAA.                                      |
| Step 3 | <b>aaa authentication login default local</b> | Set the login authorization to default to local. |

|        | Command                                                                     | Purpose                                                                                                                 |
|--------|-----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| Step 4 | <b>aaa authorization exec local</b>                                         | Configure user AAA authorization for all network-related service requests, including SLIP, PPP NCPs, and ARA protocols. |
| Step 5 | <b>aaa authorization network local</b>                                      | Configure user AAA authorization to determine if the user is allowed to run an EXEC shell.                              |
| Step 6 | <b>username <i>name</i> password <i>password</i> privilege <i>level</i></b> | Enter the local database.<br>Repeat this command for each user.                                                         |

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## Configuring the Switch for Remote Monitoring

You can use the Remote Monitoring (RMON) feature with the SNMP agent in the switch to monitor all the traffic flowing among switches on all connected LAN segments.

You can configure your switch for RMON, which is disabled by default, by using the CLI or an SNMP-compatible network management station. You cannot configure it by using VSM. In addition, a generic RMON console application is recommended on the CMS to take advantage of RMON's network management capabilities. You must also configure SNMP on the switch to access RMON MIB objects.

RMON data is usually placed in the high-priority queue for the processor and can render the switch unusable; however, because the 2950 switches use hardware counters, the monitoring is more efficient and little processing power is required.

The switch supports the following four RMON groups:

- Alarms—Monitor a specific MIB object for a specified interval, trigger an alarm at a specified value (rising threshold), and reset the alarm at another value (falling threshold). Alarms can be used with events; the alarm triggers an event, which can generate a log entry or an SNMP trap.
- Events—Determine the action to take when an event is triggered by an alarm. The action can be to generate a log entry or an SNMP trap.



- History—Collect a history group of statistics on an interface for a specified polling interval.
- Statistics—Collect Ethernet statistics on an interface.

You configure RMON alarms and events in global configuration mode by using the **rmon** alarms and **rmon** events commands. You can collect group history or group Ethernet statistics in the interface configuration mode by using the **rmon** collection history or **rmon** collection stats commands.

This guide describes the use of IOS commands that have been created or changed for switches that support IOS Release 12.0(5)WC(1). For information on other IOS Release 12.0 commands, refer to the Cisco IOS Release 12.0 documentation set available on Cisco.com.





## Creating and Maintaining VLANs

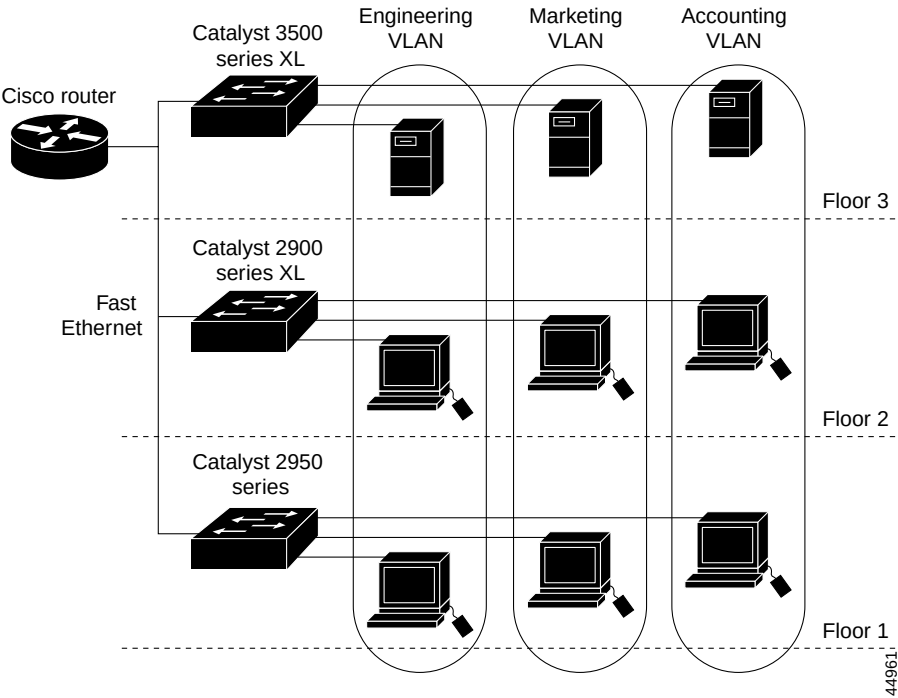
---

A virtual LAN (VLAN) is a switched network that is logically segmented by function, project team, or application, without regard to the physical locations of the users. Any switch port can belong to a VLAN, and unicast, broadcast, and multicast packets are forwarded and flooded only to stations in the VLAN. Each VLAN is considered a logical network, and packets destined for stations that do not belong to the VLAN must be forwarded through a router or bridge as shown in [Figure 5-1](#). Because a VLAN is considered a separate logical network, it contains its own bridge Management Information Base (MIB) information and can support its own implementation of the Spanning Tree Protocol (STP).

This chapter describes how to create and maintain VLANs through the Cluster Management software and the command-line interface (CLI). It contains the following information:

- How to configure static-access ports without having the VLAN Trunk Protocol (VTP) database globally propagate VLAN configuration information.
- How VTP works and how to configure its domain name, modes, and version.
- How to add, modify, and remove VLANs with different media characteristics to and from the VTP database.
- How to configure Fast Ethernet and Gigabit Ethernet VLAN trunks on a switch. The switch supports IEEE 802.1Q trunking standards for transmitting VLAN traffic. This section describes how to configure the allowed-VLAN list, the native VLAN for untagged traffic, and two methods of load sharing.
- How to configure IEEE 802.1p class of service (CoS) port priorities for port forwarding untagged frames. You assign CoS to certain types of traffic to give them priority over other traffic.

Figure 5-1 VLANs as Logically Defined Networks



# Number of Supported VLANs

Table 5-1 lists the number of supported VLANs on Catalyst 2950 switches.

Table 5-1 Number of Supported VLANs

| Catalyst Switch                  | Number of Supported VLANs | Trunking Supported? |
|----------------------------------|---------------------------|---------------------|
| 2950 switches with 16 MB of DRAM | 64                        | Yes                 |

VLANs are identified with a number between 1 and 1001. Regardless of the switch model, only 64 STP instances are supported.

The switches in [Table 5-1](#) support IEEE 802.1Q trunking methods for transmitting VLAN traffic over 100BaseT, 100BaseFX, and Gigabit Ethernet ports.

## VLAN Port Membership Modes

You configure a port to belong to a VLAN by assigning a membership mode that determines the kind of traffic the port carries and the number of VLANs it can belong to. [Table 5-2](#) lists the membership modes and characteristics.

**Table 5-2 Port Membership Modes**

| Membership Mode     | VLAN Membership Characteristics                                                                                                                                                                                                                                                                                                                              |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Static-access       | A static-access port can belong to one VLAN and is manually assigned. By default, all ports are static-access ports assigned to VLAN 1.                                                                                                                                                                                                                      |
| Trunk (IEEE 802.1Q) | A trunk is a member of all VLANs in the VLAN database by default, but membership can be limited by configuring the allowed-VLAN list.<br><br>VTP maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs on a network-wide basis. VTP exchanges VLAN configuration messages with other switches over trunk links. |

When a port belongs to a VLAN, the switch learns and manages the addresses associated with the port on a per-VLAN basis. For more information, see the [“Managing the MAC Address Tables”](#) section on page 4-49.

## VLAN Membership Combinations

You can configure your switch ports in various VLAN membership combinations as listed in [Table 5-3](#).

**Table 5-3 VLAN Combinations**

| Port Mode                     | VTP Required? | Configuration Procedure                                                                                                                                                                                                                                                                                                                                                            | Comments                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Static-access ports           | No            | <a href="#">“Assigning Static-Access Ports to a VLAN” section on page 5-5</a>                                                                                                                                                                                                                                                                                                      | If you do not want to use VTP to globally propagate the VLAN configuration information, you can assign a static-access port to a VLAN and set the VTP mode to transparent to disable VTP.                                                                                                                                                                                                                                                                                    |
| Static-access and trunk ports | Recommended   | <a href="#">“CLI: Configuring VTP Server Mode” section on page 5-14</a><br>Add, modify, or remove VLANs in the database as described in the <a href="#">“Configuring VLANs in the VTP Database” section on page 5-24</a><br><a href="#">“CLI: Assigning Static-Access Ports to a VLAN” section on page 5-28</a><br><a href="#">“Configuring a Trunk Port” section on page 5-31</a> | Make sure to configure at least one trunk port on the switch and that this trunk port is connected to the trunk port of a second switch.<br><br>Some restrictions apply to trunk ports. For more information, see the <a href="#">“Trunks Interacting with Other Features” section on page 5-30</a> .<br><br>You can change the VTP version on the switch.<br><br>You can define the allowed-VLAN list and configure the native VLAN for untagged traffic on the trunk port. |

## Clusters, VLAN Membership, and the Management VLAN

This software release supports the grouping of switches into a cluster that can be managed as a single entity. The command switch is the single point of management for the cluster and cluster members.

Links among a command switch, cluster members, and candidate switches must be through ports that belong to the management VLAN. By default, the management VLAN is VLAN 1. If you are using SNMP or the Cluster Management Suite (CMS) to manage the switch, ensure that the port through

which you are connected to a switch is in the management VLAN. For information on configuring the management VLAN, see the [“Changing the Management VLAN” section on page 3-34](#).

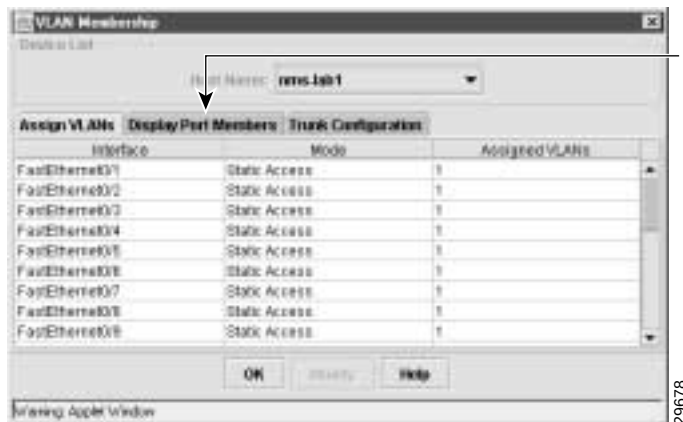
If you are configuring VLANs on a member switch, you might need to enter an extra command from the command-switch CLI to access the member switch. When configuring port parameters, for example, you can use the privileged EXEC **rcommand** command and the number of the member switch to display the member-switch CLI. Once you have accessed the member switch, command mode changes, and IOS commands operate as usual. Enter **exit** on the member switch in privileged EXEC mode to return to the command-switch CLI.

For more information about the **rcommand** command, refer to the *Catalyst 2950 Desktop Switch Command Reference*.

## Assigning Static-Access Ports to a VLAN

By default, all ports are static-access ports assigned to the management VLAN, VLAN 1.

You can assign a static-access port to a VLAN without having VTP globally propagate VLAN configuration information (VTP is disabled). To assign a VLAN, you access the VLAN Membership window ([Figure 5-2](#)) by selecting **VLAN > VLAN Membership** from the menu bar and clicking the Assign VLANs tab.

**Figure 5-2 VLAN Membership: Assign VLANs Tab**

Display the VLANs configured on a switch and the ports and membership mode of a given VLAN.

You configure the switch for VTP transparent mode, which disables VTP, by selecting **VLAN > VTP Management** from the menu bar and clicking the VTP Configuration tab (Figure 5-3).

You can also assign the port through the CLI on standalone, command, and member switches. If you are assigning a port on a cluster member to a VLAN, first log in to the member switch by using the privileged EXEC **rcommand** command. For more information on how to use this command, refer to the *Catalyst 2950 Desktop Switch Command Reference*.

## Using the VLAN Trunk Protocol

VTP is a Layer 2 messaging protocol that maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs on a network-wide basis. VTP minimizes misconfigurations and configuration inconsistencies that can cause several problems, such as duplicate VLAN names, incorrect VLAN-type specifications, and security violations.

Before you create VLANs, you must decide whether to use VTP in your network. Using VTP, you can make configuration changes centrally on a single switch, such as a Catalyst 2950, 2900 XL, or 3500 XL switch, and have those changes automatically communicated to all the other switches in the network. Without VTP, you cannot send information about VLANs to other switches.



## The VTP Domain

A VTP domain (also called a VLAN management domain) consists of one switch or several interconnected switches under the same administrative responsibility. A switch can be in only one VTP domain. You make global VLAN configuration changes for the domain by using the CLI, Cluster Management software, or Simple Network Management Protocol (SNMP).

By default, a Catalyst 2950, 2900 XL, or 3500 XL switch is in the no-management-domain state until it receives an advertisement for a domain over a trunk link (a link that carries the traffic of multiple VLANs) or until you configure a domain name. The default VTP mode is server mode, but VLAN information is not propagated over the network until a domain name is specified or learned.

If the switch receives a VTP advertisement over a trunk link, it inherits the domain name and configuration revision number. The switch then ignores advertisements with a different domain name or an earlier configuration revision number.

When you make a change to the VLAN configuration on a VTP server, the change is propagated to all switches in the VTP domain. VTP advertisements are sent over all trunk connections, including IEEE 802.1Q.

If you configure a switch for VTP transparent mode, you can create and modify VLANs, but the changes are not transmitted to other switches in the domain, and they affect only the individual switch.

For domain name and password configuration guidelines, see the [“Domain Names” section on page 5-10](#).

## VTP Modes and VTP Mode Transitions

You can configure a supported switch to be in one of the VTP modes listed in [Table 5-4](#):

**Table 5-4 VTP Modes**

| VTP Mode        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VTP server      | <p>In this mode, you can create, modify, and delete VLANs and specify other configuration parameters (such as VTP version) for the entire VTP domain. VTP servers advertise their VLAN configurations to other switches in the same VTP domain and synchronize their VLAN configurations with other switches based on advertisements received over trunk links.</p> <p>In VTP server mode, VLAN configurations are saved in nonvolatile RAM. VTP server is the default mode.</p>                                                                |
| VTP client      | <p>In this mode, a VTP client behaves like a VTP server, but you cannot create, change, or delete VLANs on a VTP client.</p> <p>In VTP client mode, VLAN configurations are saved in nonvolatile RAM.</p>                                                                                                                                                                                                                                                                                                                                       |
| VTP transparent | <p>In this mode, VTP transparent switches do not participate in VTP. A VTP transparent switch does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements. However, transparent switches do forward VTP advertisements that they receive from other switches. You can create, modify, and delete VLANs on a switch in VTP transparent mode.</p> <p>In VTP transparent mode, VLAN configurations are saved in nonvolatile RAM, but they are not advertised to other switches.</p> |

The “[VTP Configuration Guidelines](#)” section on [page 5-10](#) provides tips and caveats for configuring VTP.

## VTP Advertisements

Each switch in the VTP domain sends periodic global configuration advertisements from each trunk port to a reserved multicast address. Neighboring switches receive these advertisements and update their VTP and VLAN configurations as necessary.

**Note**

---

Because trunk ports send and receive VTP advertisements, you must ensure that at least one trunk port is configured on the switch and that this trunk port is connected to the trunk port of a second switch. Otherwise, the switch cannot receive any VTP advertisements.

---

VTP advertisements distribute the following global domain information in VTP advertisements:

- VTP domain name
- VTP configuration revision number
- Update identity and update timestamp
- MD5 digest

VTP advertisements distribute the following VLAN information for each configured VLAN:

- VLAN ID
- VLAN name
- VLAN type
- VLAN state
- Additional VLAN configuration information specific to the VLAN type

## VTP Version 2

VTP version 2 supports the following features not supported in version 1:

- Token Ring support—VTP version 2 supports Token Ring LAN switching and VLANs (Token Ring Bridge Relay Function [TrBRF] and Token Ring Concentrator Relay Function [TrCRF]). For more information about Token Ring VLANs, see the [“VLANs in the VTP Database” section on page 5-19](#).
- Unrecognized Type-Length-Value (TLV) support—A VTP server or client propagates configuration changes to its other trunks, even for TLVs it is not able to parse. The unrecognized TLV is saved in nonvolatile RAM when the switch is operating in VTP server mode.
- Version-Dependent Transparent Mode—In VTP version 1, a VTP transparent switch inspects VTP messages for the domain name and version and forwards a message only if the version and domain name match. Because only one domain is supported, VTP version 2 forwards VTP messages in transparent mode without checking the version and domain name.
- Consistency Checks—In VTP version 2, VLAN consistency checks (such as VLAN names and values) are performed only when you enter new information through the CLI, the Cluster Management software, or SNMP. Consistency checks are not performed when new information is obtained from a VTP message or when information is read from nonvolatile RAM. If the digest on a received VTP message is correct, its information is accepted without consistency checks.

## VTP Configuration Guidelines

The following sections describe the guidelines you should follow when configuring the VTP domain name, password, and the VTP version number.

### Domain Names

When configuring VTP for the first time, you must always assign a domain name. In addition, all switches in the VTP domain must be configured with the same domain name. Switches in VTP transparent mode do not exchange VTP messages with other switches, and you do not need to configure a VTP domain name for them.

**Caution**

Do not configure a VTP domain if all switches are operating in VTP client mode. If you configure the domain, it is impossible to make changes to the VLAN configuration of that domain. Therefore, make sure you configure at least one switch in the VTP domain for VTP server mode.

## Passwords

You can configure a password for the VTP domain, but it is not required. All domain switches must share the same password. Switches without a password or with the wrong password reject VTP advertisements.

**Caution**

The domain does not function properly if you do not assign the same password to each switch in the domain.

If you configure a VTP password for a domain, a Catalyst 2950, 2900 XL, or 3500 XL switch that is booted without a VTP configuration does not accept VTP advertisements until you configure it with the correct password. After the configuration, the switch accepts the next VTP advertisement that uses the same password and domain name in the advertisement.

If you are adding a new switch to an existing network that has VTP capability, the new switch learns the domain name only after the applicable password has been configured on the switch.

## VTP Version

Follow these guidelines when deciding which VTP version to implement:

- All switches in a VTP domain must run the same VTP version.
- A VTP version 2-capable switch can operate in the same VTP domain as a switch running VTP version 1 if version 2 is disabled on the version 2-capable switch (version 2 is disabled by default).

- Do not enable VTP version 2 on a switch unless all of the switches in the same VTP domain are version-2-capable. When you enable version 2 on a switch, all of the version-2-capable switches in the domain enable version 2. If there is a version 1-only switch, it will not exchange VTP information with switches with version 2 enabled.
- If there are Token Ring networks in your environment (TrBRF and TrCRF), you must enable VTP version 2 for Token Ring VLAN switching to function properly. To run Token Ring and Token Ring-Net, disable VTP version 2.

## Default VTP Configuration

Table 5-5 shows the default VTP configuration.

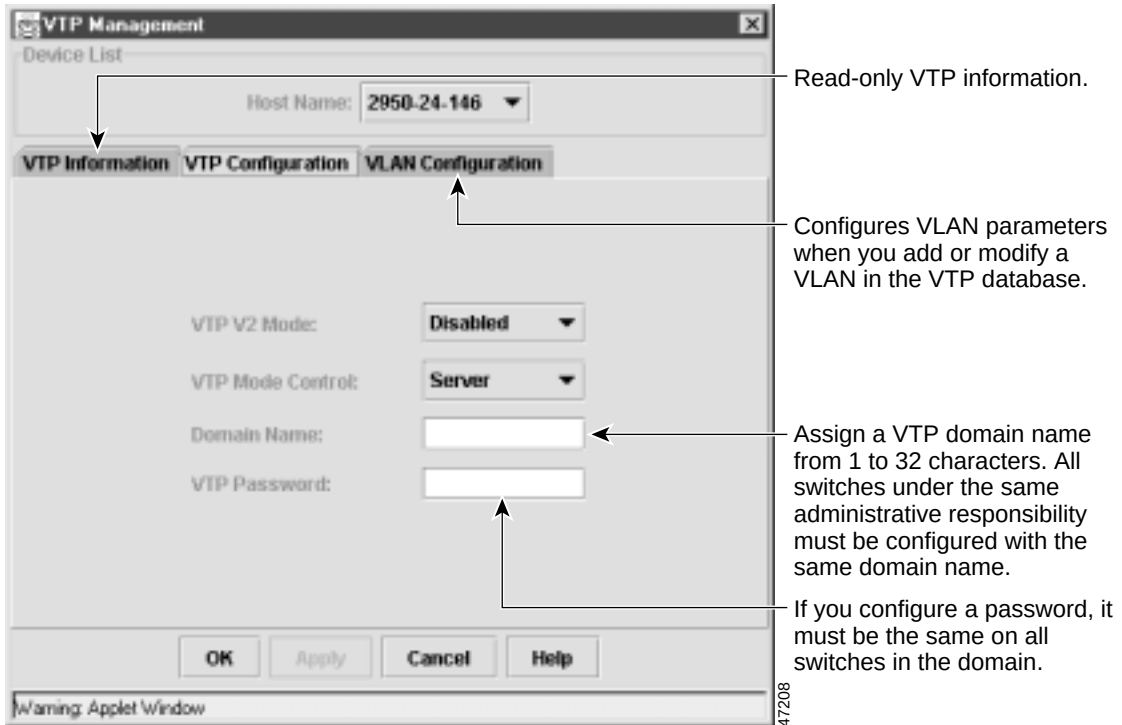
**Table 5-5 VTP Default Configuration**

| Feature                    | Default Value          |
|----------------------------|------------------------|
| VTP domain name            | Null.                  |
| VTP mode                   | Server.                |
| VTP version 2 enable state | Version 2 is disabled. |
| VTP password               | None.                  |

## Configuring VTP

You can configure VTP by using the VTP Management window (Figure 5-3).

To display this window, select **VLAN > VTP Management** from the menu bar, and click the VTP Configuration tab.

**Figure 5-3 VTP Management: VTP Configuration Tab**

After you configure VTP, you must configure a trunk port so that the switch can send and receive VTP advertisements. For more information, see the [“How VLAN Trunks Work”](#) section on page 5-29.

You can also configure VTP through the CLI on standalone, command, and member switches by entering commands in the VLAN database command mode. If you are configuring VTP on a cluster member switch to a VLAN, first log in to the member switch by using the privileged EXEC **rcommand** command. For more information on how to use this command, refer to the *Catalyst 2950 Desktop Switch Command Reference*.

When you enter the **exit** command in VLAN database mode, it applies all the commands that you entered. VTP messages are sent to other switches in the VTP domain, and you are returned to privileged EXEC mode.

**Note**

The Cisco IOS **end** and Ctrl-Z commands are not supported in VLAN database mode.

## CLI: Configuring VTP Server Mode

When a switch is in VTP server mode, you can change the VLAN configuration and have it propagated throughout the network.

Beginning in privileged EXEC mode, follow these steps to configure the switch for VTP server mode:

|        | Command                                   | Purpose                                                                                                                                                                                                                                           |
|--------|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>vlan database</b>                      | Enter VLAN database mode.                                                                                                                                                                                                                         |
| Step 2 | <b>vtp domain</b> <i>domain-name</i>      | Configure a VTP administrative-domain name.<br><br>The name can be from 1 to 32 characters.<br><br>All switches operating in VTP server or client mode under the same administrative responsibility must be configured with the same domain name. |
| Step 3 | <b>vtp password</b> <i>password-value</i> | (Optional) Set a password for the VTP domain. The password can be from 8 to 64 characters.<br><br>If you configure a VTP password, the VTP domain does not function properly if you do not assign the same password to each switch in the domain. |
| Step 4 | <b>vtp server</b>                         | Configure the switch for VTP server mode (the default).                                                                                                                                                                                           |
| Step 5 | <b>exit</b>                               | Return to privileged EXEC mode.                                                                                                                                                                                                                   |
| Step 6 | <b>show vtp status</b>                    | Verify the VTP configuration.<br><br>In the display, check the VTP Operating Mode and the VTP Domain Name fields.                                                                                                                                 |



The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## CLI: Configuring VTP Client Mode

When a switch is in VTP client mode, you cannot change its VLAN configuration. The client switch receives VTP updates from a VTP server in the VTP domain and then modifies its configuration accordingly.



### Caution

Do not configure a VTP domain name if all switches are operating in VTP client mode. If you do so, it is impossible to make changes to the VLAN configuration of that domain. Therefore, make sure you configure at least one switch as the VTP server.

Beginning in privileged EXEC mode, follow these steps to configure the switch for VTP client mode:

|        | Command                                      | Purpose                                                                                                                                                                                                                                           |
|--------|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>vlan database</b>                         | Enter VLAN database mode.                                                                                                                                                                                                                         |
| Step 2 | <b>vtp client</b>                            | Configure the switch for VTP client mode. The default setting is VTP server.                                                                                                                                                                      |
| Step 3 | <b>vtp domain</b><br><i>domain-name</i>      | Configure a VTP administrative-domain name. The name can be from 1 to 32 characters.<br><br>All switches operating in VTP server or client mode under the same administrative responsibility must be configured with the same domain name.        |
| Step 4 | <b>vtp password</b><br><i>password-value</i> | (Optional) Set a password for the VTP domain. The password can be from 8 to 64 characters.<br><br>If you configure a VTP password, the VTP domain does not function properly if you do not assign the same password to each switch in the domain. |

|        | Command                | Purpose                                                                                                          |
|--------|------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 5 | <b>exit</b>            | Update the VLAN database, propagate it throughout the administrative domain, and return to privileged EXEC mode. |
| Step 6 | <b>show vtp status</b> | Verify the VTP configuration. In the display, check the VTP Operating Mode field.                                |

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## CLI: Disabling VTP (VTP Transparent Mode)

When you configure the switch for VTP transparent mode, you disable VTP on the switch. The switch then does not send VTP updates and does not act on VTP updates received from other switches. However, a VTP transparent switch does forward received VTP advertisements on all of its trunk links.

Beginning in privileged EXEC mode, follow these steps to configure the switch for VTP transparent mode:

|        | Command                | Purpose                                                                                                                               |
|--------|------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>vlan database</b>   | Enter VLAN database mode.                                                                                                             |
| Step 2 | <b>vtp transparent</b> | Configure the switch for VTP transparent mode.<br><br>The default setting is VTP server.<br><br>This step disables VTP on the switch. |
| Step 3 | <b>exit</b>            | Return to privileged EXEC mode.                                                                                                       |
| Step 4 | <b>show vtp status</b> | Verify the VTP configuration.<br><br>In the display, check the VTP Operating Mode field.                                              |

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## CLI: Enabling VTP Version 2

VTP version 2 is disabled by default on VTP version 2-capable switches. When you enable VTP version 2 on a switch, every VTP version 2-capable switch in the VTP domain enables version 2.



### Caution

VTP version 1 and VTP version 2 are not interoperable on switches in the same VTP domain. Every switch in the VTP domain must use the same VTP version. Do not enable VTP version 2 unless every switch in the VTP domain supports version 2.



### Note

In a Token Ring environment, you must enable VTP version 2 for Token Ring VLAN switching to function properly.

For more information on VTP version configuration guidelines, see the [“VTP Version” section on page 5-11](#).

Beginning in privileged EXEC mode, follow these steps to enable VTP version 2:

|        | Command                | Purpose                                                                                                            |
|--------|------------------------|--------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>vlan database</b>   | Enter VLAN configuration mode.                                                                                     |
| Step 2 | <b>vtp v2-mode</b>     | Enable VTP version 2 on the switch.<br><br>VTP version 2 is disabled by default on VTP version 2-capable switches. |
| Step 3 | <b>exit</b>            | Update the VLAN database, propagate it throughout the administrative domain, and return to privileged EXEC mode.   |
| Step 4 | <b>show vtp status</b> | Verify that VTP version 2 is enabled.<br><br>In the display, check the VTP V2 Mode field.                          |

The [“Finding More Information About IOS Commands” section on page 4-1](#) contains the path to the complete IOS documentation.

## CLI: Disabling VTP Version 2

Beginning in privileged EXEC mode, follow these steps to disable VTP version 2:

|        | Command                | Purpose                                                                                                          |
|--------|------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>vlan database</b>   | Enter VLAN configuration mode.                                                                                   |
| Step 2 | <b>no vtp v2-mode</b>  | Disable VTP version 2.                                                                                           |
| Step 3 | <b>exit</b>            | Update the VLAN database, propagate it throughout the administrative domain, and return to privileged EXEC mode. |
| Step 4 | <b>show vtp status</b> | Verify that VTP version 2 is disabled.<br><br>In the display, check the VTP V2 Mode field.                       |

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## CLI: Monitoring VTP

You monitor VTP by displaying its configuration information: the domain name, the current VTP revision, and the number of VLANs. You can also display statistics about the advertisements sent and received by the switch.

Beginning in privileged EXEC mode, follow these steps to monitor VTP activity:

|        | Command                  | Purpose                                                      |
|--------|--------------------------|--------------------------------------------------------------|
| Step 1 | <b>show vtp status</b>   | Display the VTP switch configuration information.            |
| Step 2 | <b>show vtp counters</b> | Display counters about VTP messages being sent and received. |

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

# VLANs in the VTP Database

You can set the following parameters when you add a new VLAN to or modify an existing VLAN in the VTP database:

- VLAN ID
- VLAN name
- VLAN type (Ethernet, Fiber Distributed Data Interface [FDDI], FDDI network entity title [NET], TrBRF, or TrCRF, Token Ring, Token Ring-Net)
- VLAN state (active or suspended)
- Maximum transmission unit (MTU) for the VLAN
- Security Association Identifier (SAID)
- Bridge identification number for TrBRF VLANs
- Ring number for FDDI and TrCRF VLANs
- Parent VLAN number for TrCRF VLANs
- Spanning Tree Protocol (STP) type for TrCRF VLANs
- VLAN number to use when translating from one VLAN type to another

The [“Default VLAN Configuration” section on page 5-21](#) lists the default values and possible ranges for each VLAN media type.

## Token Ring VLANs

Although the 2950, 2900 XL, and 3500 XL switches do not support Token Ring connections, a remote device such as a Catalyst 5000 series switch with Token Ring connections could be managed from one of the supported switches. Switches running this IOS release advertise information about the following Token Ring VLANs when running VTP version 2:

- Token Ring TrBRF VLANs
- Token Ring TrCRF VLANs

For more information on configuring Token Ring VLANs, see the *Catalyst 5000 Series Software Configuration Guide*.

## VLAN Configuration Guidelines

Follow these guidelines when creating and modifying VLANs in your network:

- A maximum of 250 VLANs can be active on supported switches, but some models only support 64 VLANs. (The Catalyst 2950 switches support 64 VLANs.) If VTP reports that there are 254 active VLANs, 4 of the active VLANs (1002 to 1005) are reserved for Token Ring and FDDI.
- Before you can create a VLAN, the switch must be in VTP server mode or VTP transparent mode. For information on configuring VTP, see the [“Configuring VTP” section on page 5-12](#).
- Switches running this IOS release do not support Token Ring or FDDI media. The switch does not forward FDDI, FDDI-Net, TrCRF, or TrBRF traffic, but it does propagate the VLAN configuration through VTP.

## Default VLAN Configuration

Table 5-6 through Table 5-10 shows the default configuration for the different VLAN media types.



### Note

Catalyst 2950 switches support Ethernet interfaces exclusively. Because FDDI and Token Ring VLANs are not locally supported, you configure FDDI and Token Ring media-specific characteristics only for VTP global advertisements to other switches.

**Table 5-6 Ethernet VLAN Defaults and Ranges**

| Parameter              | Default                             | Range           |
|------------------------|-------------------------------------|-----------------|
| VLAN ID                | 1                                   | 1–1005          |
| VLAN name              | VLANxxxx, where xxxx is the VLAN ID | No range        |
| 802.10 SAID            | 100000+VLAN ID                      | 1–4294967294    |
| MTU size               | 1500                                | 1500–18190      |
| Translational bridge 1 | 0                                   | 0–1005          |
| Translational bridge 2 | 0                                   | 0–1005          |
| VLAN state             | active                              | active, suspend |

**Table 5-7 FDDI VLAN Defaults and Ranges**

| Parameter   | Default                             | Range        |
|-------------|-------------------------------------|--------------|
| VLAN ID     | 1002                                | 1–1005       |
| VLAN name   | VLANxxxx, where xxxx is the VLAN ID | No range     |
| 802.10 SAID | 100000+VLAN ID                      | 1–4294967294 |
| MTU size    | 1500                                | 1500–18190   |
| Ring number | None                                | 1–4095       |
| Parent VLAN | 0                                   | 0–1005       |

**Table 5-7 FDDI VLAN Defaults and Ranges (continued)**

| Parameter              | Default | Range           |
|------------------------|---------|-----------------|
| Translational bridge 1 | 0       | 0–1005          |
| Translational bridge 2 | 0       | 0–1005          |
| VLAN state             | active  | active, suspend |

**Table 5-8 FDDI-Net VLAN Defaults and Ranges**

| Parameter              | Default                             | Range           |
|------------------------|-------------------------------------|-----------------|
| VLAN ID                | 1004                                | 1–1005          |
| VLAN name              | VLANxxxx, where xxxx is the VLAN ID | No range        |
| 802.10 SAID            | 100000+VLAN ID                      | 1–4294967294    |
| MTU size               | 1500                                | 1500–18190      |
| Bridge number          | 0                                   | 0–15            |
| STP type               | ieee                                | auto, ibm, ieee |
| Translational bridge 1 | 0                                   | 0–1005          |
| Translational bridge 2 | 0                                   | 0–1005          |
| VLAN state             | active                              | active, suspend |

**Table 5-9 Token Ring (TrBRF) VLAN Defaults and Ranges**

| Parameter     | Default                             | Range        |
|---------------|-------------------------------------|--------------|
| VLAN ID       | 1005                                | 1–1005       |
| VLAN name     | VLANxxxx, where xxxx is the VLAN ID | No range     |
| 802.10 SAID   | 100000+VLAN ID                      | 1–4294967294 |
| MTU size      | VTPv1 1500; VTPv2 4472              | 1500–18190   |
| Bridge number | VTPv1 0; VTPv2 user-specified       | 0–15         |



**Table 5-9 Token Ring (TrBRF) VLAN Defaults and Ranges (continued)**

| Parameter              | Default | Range           |
|------------------------|---------|-----------------|
| STP type               | ibm     | auto, ibm, ieee |
| Translational bridge 1 | 0       | 0–1005          |
| Translational bridge 2 | 0       | 0–1005          |
| VLAN state             | active  | active, suspend |

**Table 5-10 Token Ring (TrCRF) VLAN Defaults and Ranges**

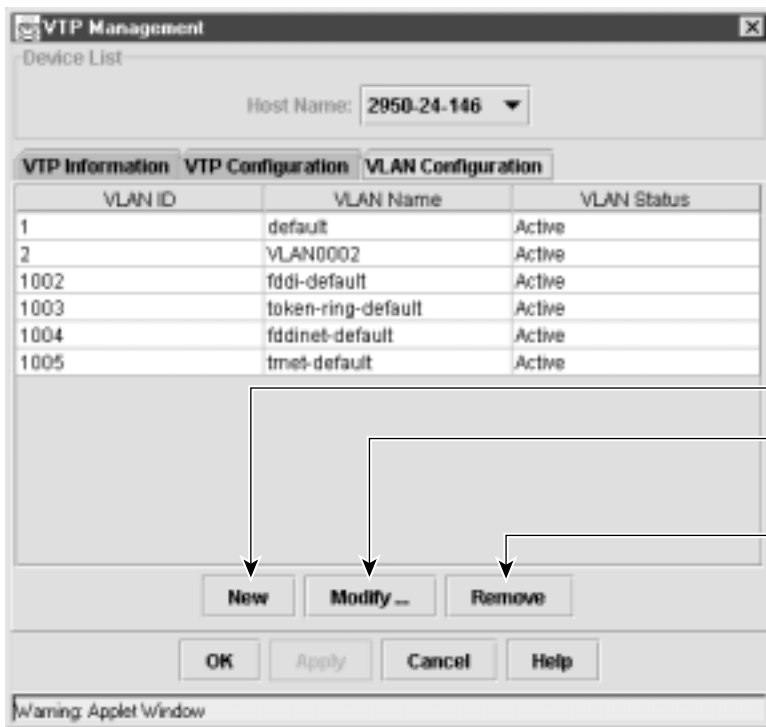
| Parameter              | Default                                | Range           |
|------------------------|----------------------------------------|-----------------|
| VLAN ID                | 1003                                   | 1–1005          |
| VLAN name              | VLANxxxx, where xxxx is the VLAN ID    | No range        |
| 802.10 SAID            | 100000+VLAN ID                         | 1–4294967294    |
| Ring Number            | VTPv1 default 0; VTPv2 user-specified  | 1–4095          |
| Parent VLAN            | VTPv1 default 0; VTPv2 user-specified  | 0–1005          |
| MTU size               | VTPv1 default 1500; VTPv2 default 4472 | 1500–18190      |
| Translational bridge 1 | 0                                      | 0–1005          |
| Translational bridge 2 | 0                                      | 0–1005          |
| VLAN state             | active                                 | active, suspend |
| Bridge mode            | srb                                    | srb, srt        |
| ARE max hops           | 7                                      | 0–13            |
| STE max hops           | 7                                      | 0–13            |
| Backup CRF             | disabled                               | disable; enable |

## Configuring VLANs in the VTP Database

You can use the VTP Management window (Figure 5-4) or the CLI to add, modify or remove VLAN configurations in the VTP database. VTP globally propagates these VLAN changes throughout the VTP domain.

To display this window, select **VLAN > VTP Management** from the menu bar, and click the VLAN Configuration tab. Click **Help** to for more information on using this window.

**Figure 5-4 VTP Management: VLAN Configuration Tab**



Add a VLAN to the database.

Select an existing VLAN, and click Modify to change its parameters.

Select a row, and click Remove to delete a VLAN from the database. You cannot remove VLANs 1 or 1002-1005.

You use the CLI **vlan database** command mode to add, change, and delete VLANs. In VTP server or transparent mode, commands to add, change, and delete VLANs are written to the file `vlan.dat`, and you can display them by entering the

privileged EXEC mode **show vlan** command. The vlan.dat file is stored in nonvolatile memory. The vlan.dat file is upgraded automatically, but you cannot return to an earlier version of Cisco IOS after you upgrade to this release.

**Caution**

---

You can cause inconsistency in the VLAN database if you attempt to manually delete the vlan.dat file. If you want to modify the VLAN configuration or VTP, use the VLAN database commands described in the *Catalyst 2950 Desktop Switch Command Reference*.

---

You use the interface configuration command mode to define the port membership mode and add and remove ports from VLAN. The results of these commands are written to the running-configuration file, and you can display the file by entering the privileged EXEC mode **show running-config command**.

**Note**

---

VLANs can be configured to support a number of parameters that are not discussed in detail in this section. For complete information on the commands and parameters that control VLAN configuration, refer to the *Catalyst 2950 Desktop Switch Command Reference*.

---

## CLI: Adding an VLAN

Each VLAN has a unique, 4-digit ID that can be a number from 1 to 1001. To add a VLAN to the VLAN database, assign a number and name to the VLAN. For the list of default parameters that are assigned when you add a VLAN, see the [“Default VLAN Configuration” section on page 5-21](#).

If you do not specify the VLAN type, the VLAN is an Ethernet VLAN.

Beginning in privileged EXEC mode, follow these steps to add an Ethernet VLAN:

|        | Command                                                 | Purpose                                                                                                                                                                                                 |
|--------|---------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>vlan database</b>                                    | Enter VLAN database mode.                                                                                                                                                                               |
| Step 2 | <b>vlan</b> <i>vlan-id</i> <b>name</b> <i>vlan-name</i> | Add an Ethernet VLAN by assigning a number to it. If no name is entered for the VLAN, the default is to append the <i>vlan-id</i> to the word VLAN. For example, VLAN0004 could be a default VLAN name. |
| Step 3 | <b>exit</b>                                             | Update the VLAN database, propagate it throughout the administrative domain, and return to privileged EXEC mode.                                                                                        |
| Step 4 | <b>show vlan name</b> <i>vlan-name</i>                  | Verify the VLAN configuration.                                                                                                                                                                          |

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## CLI: Modifying a VLAN

Beginning in privileged EXEC mode, follow these steps to modify an Ethernet VLAN:

|        | Command                                               | Purpose                                                                                                          |
|--------|-------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>vlan database</b>                                  | Enter VLAN configuration mode.                                                                                   |
| Step 2 | <b>vlan</b> <i>vlan-id</i> <b>mtu</b> <i>mtu-size</i> | Identify the VLAN, and change the MTU size.                                                                      |
| Step 3 | <b>exit</b>                                           | Update the VLAN database, propagate it throughout the administrative domain, and return to privileged EXEC mode. |
| Step 4 | <b>show vlan</b> <i>vlan-id</i>                       | Verify the VLAN configuration.                                                                                   |

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## CLI: Deleting a VLAN

When you delete a VLAN from a switch that is in VTP server mode, the VLAN is removed from all switches in the VTP domain. When you delete a VLAN from a switch that is in VTP transparent mode, the VLAN is deleted only on that specific switch.

You cannot delete the default VLANs for the different media types: Ethernet VLAN 1 and FDDI or Token Ring VLANs 1002 to 1005.

**Caution**

When you delete a VLAN, any ports assigned to that VLAN become inactive. They remain associated with the VLAN (and thus inactive) until you assign them to a new VLAN.

Beginning in privileged EXEC mode, follow these steps to delete a VLAN on the switch:

|        | Command                       | Purpose                                                                                                          |
|--------|-------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>vlan database</b>          | Enter VLAN configuration mode.                                                                                   |
| Step 2 | <b>no vlan <i>vlan-id</i></b> | Remove the VLAN by using the VLAN ID.                                                                            |
| Step 3 | <b>exit</b>                   | Update the VLAN database, propagate it throughout the administrative domain, and return to privileged EXEC mode. |
| Step 4 | <b>show vlan brief</b>        | Verify the VLAN removal.                                                                                         |

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## CLI: Assigning Static-Access Ports to a VLAN

By default, all ports are static-access ports assigned to VLAN 1, which is the default management VLAN. If you are assigning a port on a cluster member switch to a VLAN, first log in to the member switch by using the privileged EXEC **rcommand** command. For more information on how to use this command, refer to the *Cisco IOS Desktop Switching Command Reference* (online only).

Beginning in privileged EXEC mode, follow these steps to assign a port to a VLAN in the VTP database:

|        | Command                                                        | Purpose                                                                                                                                        |
|--------|----------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>                                      | Enter global configuration mode.                                                                                                               |
| Step 2 | <b>interface</b> <i>interface</i>                              | Enter interface configuration mode, and define the interface to be added to the VLAN.                                                          |
| Step 3 | <b>switchport mode access</b>                                  | Define the VLAN membership mode for this port.                                                                                                 |
| Step 4 | <b>switchport access vlan 3</b>                                | Assign the port to the VLAN.                                                                                                                   |
| Step 5 | <b>exit</b>                                                    | Return to privileged EXEC mode.                                                                                                                |
| Step 6 | <b>show interface</b> <i>interface-id</i><br><b>switchport</b> | Verify the VLAN configuration.<br><br>In the display, check the Operation Mode, Access Mode VLAN, and the Priority for Untagged Frames fields. |

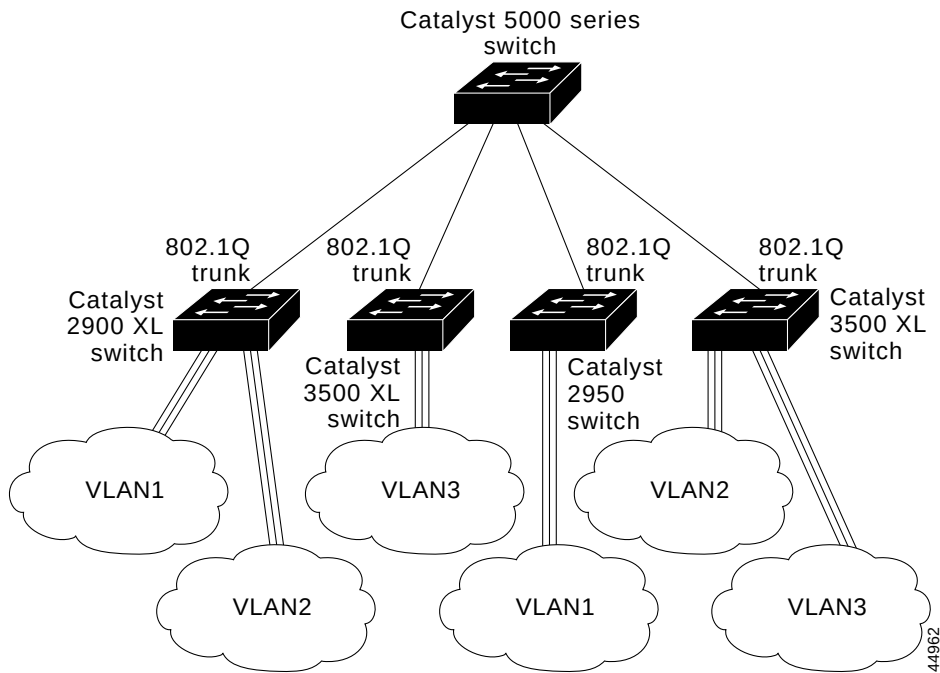
The “[Finding More Information About IOS Commands](#)” section on page 4-1 contains the path to the complete IOS documentation.

# How VLAN Trunks Work

A trunk is a point-to-point link that transmits and receives traffic between switches or between switches and routers. Trunks carry the traffic of multiple VLANs and can extend VLANs across an entire network.

Figure 5-5 shows a network of switches that are connected by 802.1Q trunks.

**Figure 5-5 Catalyst 2950, 2900 XL, and 3500 XL Switches in a 802.1Q Trunking Environment**



## IEEE 802.1Q Configuration Considerations

IEEE 802.1Q trunks impose some limitations on the trunking strategy for a network. The following restrictions apply when using 802.1Q trunks:

- Make sure the native VLAN for a 802.1Q trunk is the same on both ends of the trunk link. If the native VLAN on one end of the trunk is different from the native VLAN on the other end, spanning-tree loops might result.
- Disabling STP on the native VLAN of a 802.1Q trunk without disabling STP on every VLAN in the network can potentially cause STP loops. We recommend that you leave STP enabled on the native VLAN of a 802.1Q trunk or disable STP on every VLAN in the network. Make sure your network is loop-free before disabling STP.

## Trunks Interacting with Other Features

IEEE 802.1Q trunking interacts with other switch features as described in [Table 5-11](#).

**Table 5-11** *Trunks Interacting with Other Features*

| Switch Feature  | Trunk Port Interaction                                                                                           |
|-----------------|------------------------------------------------------------------------------------------------------------------|
| Port monitoring | A trunk port cannot be a monitor port. A static-access port can monitor the traffic of its VLAN on a trunk port. |



**Table 5-11 Trunks Interacting with Other Features (continued)**

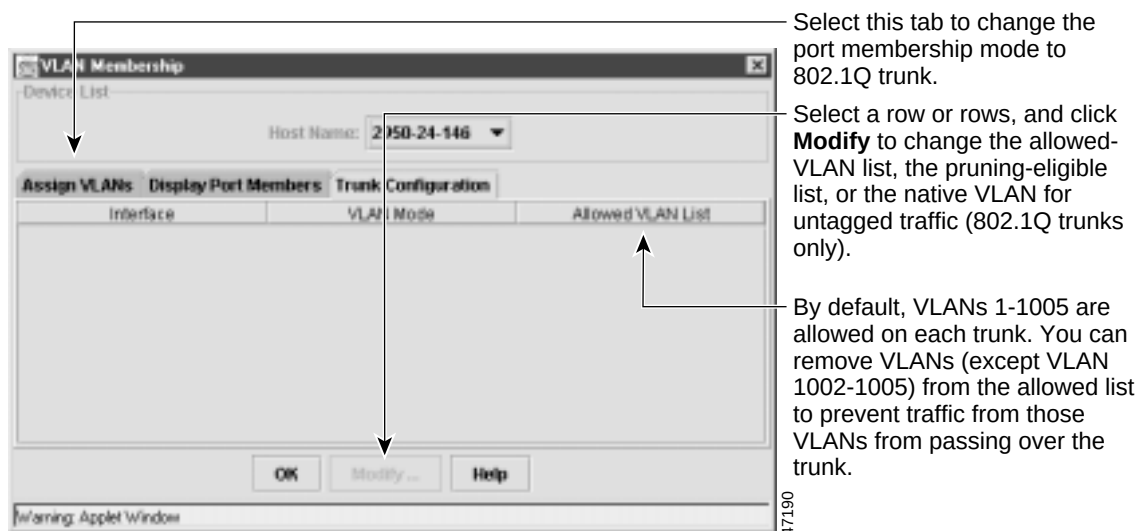
| Switch Feature | Trunk Port Interaction                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Secure ports   | A trunk port cannot be a secure port.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Port grouping  | <p>802.1Q trunks can be grouped into EtherChannel port groups, but all trunks in the group must have the same configuration.</p> <p>When a group is first created, all ports follow the parameters set for the first port to be added to the group. If you change the configuration of one of the following parameters, the switch propagates the setting you entered to all ports in the group:</p> <ul style="list-style-type: none"><li>• Allowed-VLAN list</li><li>• STP path cost for each VLAN</li><li>• STP port priority for each VLAN</li><li>• STP Port Fast setting</li><li>• Trunk status: if one port in a port group ceases to be a trunk, all port cease to be trunks.</li></ul> |

## Configuring a Trunk Port

You configure trunk ports by using the Assign VLANs (Figure 5-2) and Trunk Configuration (Figure 5-6) tabs of the VLAN Membership window.

To display this window, select **VLAN > VLAN Membership** from the menu bar. Then click the Assign VLANs tab or the Trunk Configuration tab.

Figure 5-6 VLAN Membership: Trunk Configuration Tab



You can also configure a trunk port through the CLI on standalone, command, and member switches. If you are assigning a port on a cluster member switch to a VLAN, first log in to the member switch by using the privileged EXEC **rcommand** command. For more information on how to use this command, refer to the *Catalyst 2950 Desktop Switch Command Reference*.

## CLI: Configuring a Trunk Port

For information on trunk port interactions with other features, see the [“Trunks Interacting with Other Features”](#) section on page 5-30.



### Note

Because trunk ports send and receive VTP advertisements, you must ensure that at least one trunk port is configured on the switch and that this trunk port is connected to the trunk port of a second switch. Otherwise, the switch cannot receive any VTP advertisements.

Beginning in privileged EXEC mode, follow these steps to configure a port as a 802.1Q trunk port:

|        | Command                                                        | Purpose                                                                                                                              |
|--------|----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>                                      | Enter global configuration mode.                                                                                                     |
| Step 2 | <b>interface</b> <i>interface_id</i>                           | Enter the interface configuration mode and the port to be configured for trunking.                                                   |
| Step 3 | <b>switchport mode trunk</b>                                   | Configure the port as a VLAN trunk.                                                                                                  |
| Step 4 | <b>switchport trunk encapsulation {dot1q}</b>                  | Configure the port to support 802.1Q encapsulation.<br><br>You must configure each end of the link with the same encapsulation type. |
| Step 5 | <b>end</b>                                                     | Return to privileged EXEC mode.                                                                                                      |
| Step 6 | <b>show interface</b> <i>interface-id</i><br><b>switchport</b> | Verify your entries.<br><br>In the display, check the Operational Mode and the Operational Trunking Encapsulation fields.            |
| Step 7 | <b>copy running-config startup-config</b>                      | Save the configuration.                                                                                                              |

**Note**

This software release does not support trunk negotiation through the Dynamic Trunk Protocol (DTP), formerly known as Dynamic ISL (DISL). If you are connecting a trunk port to a Catalyst 5000 switch or other DTP device, use the non-negotiate option on the DTP-capable device so that the switch port does not generate DTP frames.

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## CLI: Disabling a Trunk Port

You can disable trunking on a port by returning it to its default static-access mode. Beginning in privileged EXEC mode, follow these steps to disable trunking on a port:

|        | Command                                                        | Purpose                                                                              |
|--------|----------------------------------------------------------------|--------------------------------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>                                      | Enter global configuration mode.                                                     |
| Step 2 | <b>interface</b> <i>interface_id</i>                           | Enter the interface configuration mode and the port to be added to the VLAN.         |
| Step 3 | <b>no switchport mode</b>                                      | Return the port to its default static-access mode.                                   |
| Step 4 | <b>end</b>                                                     | Return to privileged EXEC.                                                           |
| Step 5 | <b>show interface</b> <i>interface-id</i><br><b>switchport</b> | Verify your entries.<br><br>In the display, check the Negotiation of Trunking field. |

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## CLI: Defining the Allowed VLANs on a Trunk

By default, a trunk port sends to and receives traffic from all VLANs in the VLAN database. All VLANs, 1 to 1005, are allowed on each trunk. However, you can remove VLANs from the allowed list, preventing traffic from those VLANs from passing over the trunk. To restrict the traffic a trunk carries, use the **remove vlan-list** parameter to remove specific VLANs from the allowed list.

A trunk port can become a member of a VLAN if the VLAN is enabled, if VTP knows of the VLAN, and if the VLAN is in the allowed list for the port. When VTP detects a newly enabled VLAN and the VLAN is in the allowed list for a trunk port, the trunk port automatically becomes a member of the enabled VLAN. When VTP detects a new VLAN and the VLAN is not in the allowed list for a trunk port, the trunk port does not become a member of the new VLAN.

Beginning in privileged EXEC mode, follow these steps to modify the allowed list of a 802.1Q trunk:

|        | Command                                                                     | Purpose                                                                                                                                                                                                                                                                              |
|--------|-----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>                                                   | Enter global configuration mode.                                                                                                                                                                                                                                                     |
| Step 2 | <b>interface</b> <i>interface_id</i>                                        | Enter interface configuration mode and the port to be added to the VLAN.                                                                                                                                                                                                             |
| Step 3 | <b>switchport mode trunk</b>                                                | Configure VLAN membership mode for trunks.                                                                                                                                                                                                                                           |
| Step 4 | <b>switchport trunk allowed<br/>vlan remove</b> <i>vlan-list</i>            | Define the VLANs that are <i>not</i> allowed to transmit and receive on the port.<br><br>The <i>vlan-list</i> parameter is a range of VLAN IDs. Separate nonconsecutive VLAN IDs with a comma and no spaces; use a hyphen to designate a range of IDs. Valid IDs are from 2 to 1001. |
| Step 5 | <b>end</b>                                                                  | Return to privileged EXEC.                                                                                                                                                                                                                                                           |
| Step 6 | <b>show interface</b> <i>interface-id</i><br><b>switchport allowed-vlan</b> | Verify your entries.                                                                                                                                                                                                                                                                 |
| Step 7 | <b>copy running-config<br/>startup-config</b>                               | Save the configuration.                                                                                                                                                                                                                                                              |

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## CLI: Configuring the Native VLAN for Untagged Traffic

A trunk port configured with 802.1Q tagging can receive both tagged and untagged traffic. By default, the switch forwards untagged traffic with the native VLAN configured for the port. The native VLAN is VLAN 1 by default.



**Note**

The native VLAN can be assigned any VLAN ID, and it is not dependent on the management VLAN.

For information about 802.1Q configuration issues, see the [“IEEE 802.1Q Configuration Considerations” section on page 5-30](#).

Beginning in privileged EXEC mode, follow these steps to configure the native VLAN on a 802.1Q trunk:

|        | Command                                                        | Purpose                                                                                                               |
|--------|----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>                                      | Enter global configuration mode.                                                                                      |
| Step 2 | <b>interface</b> <i>interface-id</i>                           | Enter interface configuration mode, and define the interface that is configured as the 802.1Q trunk.                  |
| Step 3 | <b>switchport trunk native vlan</b> <i>vlan-id</i>             | Configure the VLAN that is sending and receiving untagged traffic on the trunk port.<br>Valid IDs are from 1 to 1001. |
| Step 4 | <b>show interface</b> <i>interface-id</i><br><b>switchport</b> | Verify your settings.                                                                                                 |

If a packet has a VLAN ID the same as the outgoing port native VLAN ID, the packet is transmitted untagged; otherwise, the switch transmits the packet with a tag.

The [“Finding More Information About IOS Commands” section on page 4-1](#) contains the path to the complete IOS documentation.

## Configuring IEEE 802.1p Class of Service

The Catalyst 2950 switches provide QoS-based 802.1p class of service (CoS) values. QoS uses classification and scheduling to transmit network traffic from the switch in a predictable manner. QoS classifies frames by assigning priority-indexed CoS values to them and gives preference to higher-priority traffic such as telephone calls.

### How Class of Service Works

Before you set up 802.1p CoS on a Catalyst 2950, 2900 XL, and 3500 XL switch that operates with the Catalyst 6000 family of switches, refer to the Catalyst 6000 documentation. There are differences in the 802.1p implementation, and they should be understood to ensure compatibility.

### Port Priority

Frames received from users in the administratively-defined VLANs are classified or *tagged* for transmission to other devices. Based on rules you define, a unique identifier (the tag) is inserted in each frame header before it is forwarded. The tag is examined and understood by each device before any broadcasts or transmissions to other switches, routers, or end stations. When the frame reaches the last switch or router, the tag is removed before the frame is transmitted to the target end station. VLANs that are assigned on trunk or access ports without identification or a tag are called *native* or *untagged* frames.

For IEEE 802.1Q frames with tag information, the priority value from the header frame is used. For native frames, the default priority of the input port is used.

### Port Scheduling

Each port on the switch has a single receive queue buffer (the *ingress* port) for incoming traffic. When an untagged frame arrives, it is assigned the value of the port as its port default priority. You assign this value by using the CLI or CMS software. A tagged frame continues to use its assigned CoS value when it passes through the ingress port.

CoS configures each transmit port (the *egress* port) with a normal-priority transmit queue and a high-priority transmit queue, depending on the frame tag or the port information. Frames in the normal-priority queue are forwarded only after frames in the high-priority queue are forwarded.

Table 5-12 shows the two categories of switch transmit queues.

**Table 5-12 Transmit Queue Information**

| Transmit queue category <sup>1</sup>                              | Transmit Queues                                                                                                                                                    |
|-------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2950 switches (802.1p user priority)                              | There are four priority queues. The frames are forwarded to appropriate queues based on priority-to-queue mapping as defined by the user.                          |
| 2900 XL switches, 2900 XL Ethernet modules (802.1p user priority) | Frames with a priority value of 0 through 3 are sent to a normal-priority queue.<br>Frames with a priority value of 4 through 7 are sent to a high-priority queue. |
| 3500 XL switches, Gigabit Ethernet modules (802.1p user priority) | Frames with a priority value of 0 through 3 are sent to a normal-priority queue.<br>Frames with a priority value of 4 through 7 are sent to a high-priority queue. |

1. Catalyst 2900 XL switches with 4 MB of DRAM and the WS-X2914-XL and the WS-X2922-XL modules only have one transmit queue and do not support QoS.

## CLI: Configuring the CoS Port Priorities

Beginning in privileged EXEC mode, follow these steps to set the port priority for untagged (native) Ethernet frames:

|        | Command                                                          | Purpose                                                                                                            |
|--------|------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>                                        | Enter global configuration mode.                                                                                   |
| Step 2 | <b>interface</b> <i>interface</i>                                | Enter the interface to be configured.                                                                              |
| Step 3 | <b>switchport priority default</b><br><i>default-priority-id</i> | Set the port priority on the interface.<br>Frames are forwarded to appropriate queues as per CoS to queue mapping. |



|        | Command                                                        | Purpose                                                                            |
|--------|----------------------------------------------------------------|------------------------------------------------------------------------------------|
| Step 4 | <b>end</b>                                                     | Return to privileged EXEC mode.                                                    |
| Step 5 | <b>show interface</b> <i>interface-id</i><br><b>switchport</b> | Verify your entries. In the display, check the Priority for Untagged Frames field. |

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## CoS and WRR

The Catalyst 2950 switches support four CoS queues for each egress port. For each queue, you can specify the following types of scheduling:

- Strict priority scheduling

Strict priority scheduling is based on the priority of queues. Packets can have priorities from 0 to 7, 7 being the highest. Packets in the high-priority queue always transmit first, and packets in the low-priority queue do not transmit until all the high-priority queues become empty.

- Weighted round-robin (WRR) scheduling

WRR scheduling requires you to specify a number that indicates the importance (weight) of the queue relative to the other CoS queues. WRR scheduling prevents the low-priority queues from being completely neglected during periods of high-priority traffic. The WRR scheduler transmits some packets from each queue in turn. The number of packets it transmits corresponds to the relative importance of the queue. For example, if one queue has a weight of 3 and another has a weight of 4, then three packets are transmitted from the first queue for every four that are transmitted from the second queue. By using this scheduling, low-priority queues have the opportunity to transmit packets even though the high-priority queues are not empty.

Use the CoS and WRR window ([Figure 5-7](#)) to assign priorities to the queues and to enable the WRR scheduler. To display this window, select **Device > CoS & WRR** from the menu bar.

You can use this window to perform the following tasks:

- Enable or disable WRR
- Assign packets to queues based on priority

- Assign relative weights to the output queues

Use the **CoS** tab on the CoS and WRR window (Figure 5-7) to view the default settings. If you want to reassign a priority, open the list under that priority, and select a different queue number.

**Figure 5-7 Modify CoS Settings**

**CoS & WRR**

Device List

Host Name: 2950-24-146

**CoS** **WRR**

| CoS         | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|-------------|---|---|---|---|---|---|---|---|
| Queue (1-4) | 1 | 2 | 2 | 2 | 3 | 3 | 4 | 1 |

Default

OK Apply Cancel Help

Warning: Applet Window

47210

Use the **WRR** tab on the CoS and WRR window (Figure 5-8) to view the current settings. If WRR scheduler is disabled, all the fields will be blank.

If the WRR priority box is checked, WRR is enabled. You can assign a weighted number from 0 to 255 in the field below each queue number, as shown in Figure 5-8.

**Figure 5-8** Modify WRR Settings

**CoS & WRR**

Device List

Host Name: 2950-24-146 ▼

**CoS** **WRR**

☐ Enable Weighted Round Robin priority

| Queue       | 1                    | 2                    | 3                    | 4                    |
|-------------|----------------------|----------------------|----------------------|----------------------|
| WRR (1-255) | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |

OK Apply Cancel Help

Warning: Applet Window

4/2/11

## CLI: Configuring CoS Priority Queues

Beginning in privileged EXEC mode, follow these steps to configure the CoS priority queues:

|           | Command                                        | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                      |           |                     |      |   |      |   |      |   |      |   |
|-----------|------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|---------------------|------|---|------|---|------|---|------|---|
| Step 1    | <b>configure terminal</b>                      | Enter global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                             |           |                     |      |   |      |   |      |   |      |   |
| Step 2    | <b>wrr-queue cos-map</b> <i>qid cos1..cosn</i> | <p>Specify the queue id of the CoS priority queue. (Ranges are 1 to 4 where 1 is the lowest CoS priority queue.)</p> <p>Specify the CoS values that are mapped to queue id.</p> <p>Default values are as follows:</p> <table><tr><th>CoS Value</th><th>CoS Priority Queues</th></tr><tr><td>0, 1</td><td>1</td></tr><tr><td>2, 3</td><td>2</td></tr><tr><td>4, 5</td><td>3</td></tr><tr><td>6, 7</td><td>4</td></tr></table> | CoS Value | CoS Priority Queues | 0, 1 | 1 | 2, 3 | 2 | 4, 5 | 3 | 6, 7 | 4 |
| CoS Value | CoS Priority Queues                            |                                                                                                                                                                                                                                                                                                                                                                                                                              |           |                     |      |   |      |   |      |   |      |   |
| 0, 1      | 1                                              |                                                                                                                                                                                                                                                                                                                                                                                                                              |           |                     |      |   |      |   |      |   |      |   |
| 2, 3      | 2                                              |                                                                                                                                                                                                                                                                                                                                                                                                                              |           |                     |      |   |      |   |      |   |      |   |
| 4, 5      | 3                                              |                                                                                                                                                                                                                                                                                                                                                                                                                              |           |                     |      |   |      |   |      |   |      |   |
| 6, 7      | 4                                              |                                                                                                                                                                                                                                                                                                                                                                                                                              |           |                     |      |   |      |   |      |   |      |   |
| Step 3    | <b>end</b>                                     | Return to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                              |           |                     |      |   |      |   |      |   |      |   |
| Step 4    | <b>show cos-map</b>                            | Display the mapping of the CoS priority queues.                                                                                                                                                                                                                                                                                                                                                                              |           |                     |      |   |      |   |      |   |      |   |

To disable the new CoS settings and return to default settings, use the **no wrr-queue cos-map** command.

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## CLI: Configuring WRR

Beginning in privileged EXEC mode, follow these steps to configure the weighted round robin priority:

|        | Command                                                | Purpose                                                                              |
|--------|--------------------------------------------------------|--------------------------------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>                              | Enter global configuration mode.                                                     |
| Step 2 | <b>wrr-queue bandwidth</b><br><i>weight1...weight4</i> | Assign WRR weights to the four CoS queues. (Ranges for the WRR values are 1 to 255.) |
| Step 3 | <b>end</b>                                             | Return to privileged EXEC mode.                                                      |
| Step 4 | <b>show wrr-queue bandwidth</b>                        | Display the WRR bandwidth allocation for the CoS priority queues.                    |

To disable the WRR scheduler and enable the strict priority scheduler, use the **no wrr-queue bandwidth** command.

The [“Finding More Information About IOS Commands” section on page 4-1](#) contains the path to the complete IOS documentation.

## Load Sharing Using STP

Load sharing divides the bandwidth supplied by parallel trunks connecting switches. To avoid loops, STP normally blocks all but one parallel link between switches. With load sharing, you divide the traffic between the links according to which VLAN the traffic belongs.

You configure load sharing on trunk ports by using STP port priorities or STP path costs. For load sharing using STP port priorities, both load-sharing links must be connected to the same switch. For load sharing using STP path costs, each load-sharing link can be connected to the same switch or to two different switches.

You can change STP port parameters by using the Port Parameters tab of the Spanning Tree Protocol window or by using the CLI. To display this window, select **Device > Spanning-Tree Protocol** from the menu bar. Then click the **Port Parameters** tab.

For more information about the STP window, see the [“Configuring the Spanning Tree Protocol” section on page 4-80](#), or consult the online help in the application.

## Load Sharing Using STP Port Priorities

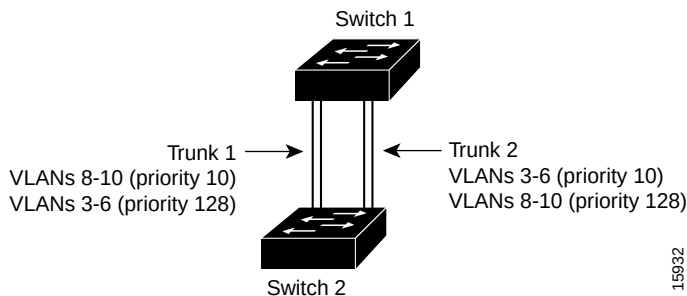
When two ports on the same switch form a loop, the STP port priority setting determines which port is enabled and which port is in standby mode. You can set the priorities on a parallel trunk port so that the port carries all the traffic for a given VLAN. The trunk port with the higher priority (lower values) for a VLAN is forwarding traffic for that VLAN. The trunk port with the lower priority (higher values) for the same VLAN remains in a blocking state for that VLAN. One trunk port transmits or receives all traffic for the VLAN.

[Figure 5-9](#) shows two trunks connecting supported switches. In this example, the switches are configured as follows:

- VLANs 8 through 10 are assigned a port priority of 10 on trunk 1.
- VLANs 3 through 6 retain the default port priority of 128 on trunk 1.
- VLANs 3 through 6 are assigned a port priority of 10 on trunk 2.
- VLANs 8 through 10 retain the default port priority of 128 on trunk 2.

In this way, trunk 1 carries traffic for VLANs 8 through 10, and trunk 2 carries traffic for VLANs 3 through 6. If the active trunk fails, the trunk with the lower priority takes over and carries the traffic for all of the VLANs. No duplication of traffic occurs over any trunk port.

**Figure 5-9 Load Sharing by Using STP Port Priorities**



15932

## CLI: Configuring STP Port Priorities and Load Sharing

Beginning in privileged EXEC mode, follow these steps to configure the network shown in [Figure 5-9](#):

|         | Command                                | Purpose                                                                                                                                         |
|---------|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1  | <b>vlan database</b>                   | On Switch 1, enter VLAN configuration mode.                                                                                                     |
| Step 2  | <b>vtp domain</b> <i>domain-name</i>   | Configure a VTP administrative domain.<br>The domain name can be from 1 to 32 characters.                                                       |
| Step 3  | <b>vtp server</b>                      | Configure Switch 1 as the VTP server.                                                                                                           |
| Step 4  | <b>exit</b>                            | Return to privileged EXEC mode.                                                                                                                 |
| Step 5  | <b>show vtp status</b>                 | Verify the VTP configuration on both Switch 1 and Switch 2.<br><br>In the display, check the VTP Operating Mode and the VTP Domain Name fields. |
| Step 6  | <b>show vlan</b>                       | Verify that the VLANs exist in the database on Switch 1.                                                                                        |
| Step 7  | <b>configure terminal</b>              | Enter global configuration mode.                                                                                                                |
| Step 8  | <b>interface fa0/1</b>                 | Enter interface configuration mode, and define Fa0/1 as the interface to be configured as a trunk.                                              |
| Step 9  | <b>switchport mode trunk</b>           | Configure the port as a trunk port.                                                                                                             |
| Step 10 | <b>end</b>                             | Return to privilege EXEC mode.                                                                                                                  |
| Step 11 | <b>show interface fa0/1 switchport</b> | Verify the VLAN configuration.                                                                                                                  |
| Step 12 |                                        | Repeat Steps 7 through 11 on Switch 1 for interface Fa0/2.                                                                                      |
| Step 13 |                                        | Repeat Steps 7 through 11 on Switch 2 to configure the trunk ports on interface Fa0/1 and Fa0/2.                                                |

|         | Command                                            | Purpose                                                                                                                                    |
|---------|----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| Step 14 | <b>show vlan</b>                                   | When the trunk links come up, VTP passes the VTP and VLAN information to Switch 2. Verify the Switch 2 has learned the VLAN configuration. |
| Step 15 | <b>configure terminal</b>                          | Enter global configuration mode on Switch 1.                                                                                               |
| Step 16 | <b>interface fa0/1</b>                             | Enter interface configuration mode, and define the interface to set the STP port priority.                                                 |
| Step 17 | <b>spanning-tree vlan 8 9 10 port-priority 10</b>  | Assign the port priority of 10 for VLANs 8, 9, and 10.                                                                                     |
| Step 18 | <b>end</b>                                         | Return to global configuration mode.                                                                                                       |
| Step 19 | <b>interface fa0/2</b>                             | Enter interface configuration mode, and define the interface to set the STP port priority.                                                 |
| Step 20 | <b>spanning-tree vlan 3 4 5 6 port priority 10</b> | Assign the port priority of 10 for VLANs 3, 4, 5, and 6.                                                                                   |
| Step 21 | <b>exit</b>                                        | Return to privileged EXEC mode.                                                                                                            |
| Step 22 | <b>show running-config</b>                         | Verify your entries.                                                                                                                       |

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation.

## Load Sharing Using STP Path Cost

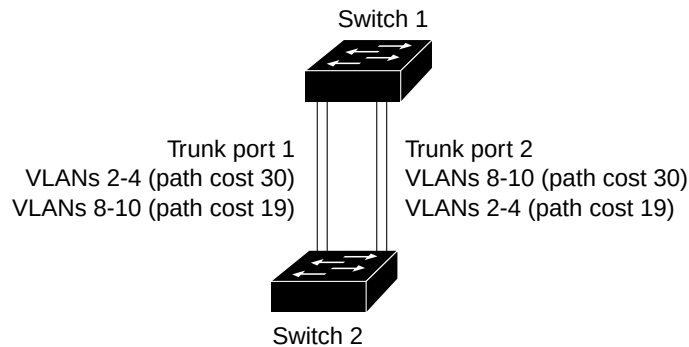
You can configure parallel trunks to share VLAN traffic by setting different path costs on a trunk and associating the path costs with different sets of VLANs. The VLANs keep the traffic separate, because no loops exist, STP does not disable the ports, and redundancy is maintained in the event of a lost link.



In [Figure 5-10](#), trunk ports 1 and 2 are 100BaseT ports. The path costs for the VLANs are assigned as follows:

- VLANs 2 through 4 are assigned a path cost of 30 on trunk port 1.
- VLANs 8 through 10 retain the default 100BaseT path cost on trunk port 1 of 19.
- VLANs 8 through 10 are assigned a path cost of 30 on trunk port 2.
- VLANs 2 through 4 retain the default 100BaseT path cost on trunk port 2 of 19.

**Figure 5-10 Load-Sharing Trunks with Traffic Distributed by Path Cost**



16591

## CLI: Configuring STP Path Costs and Load Sharing

Beginning in privileged EXEC mode, follow these steps to configure the network shown in [Figure 5-10](#):

|         | Command                                 | Purpose                                                                                                                                               |
|---------|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1  | <b>configure terminal</b>               | Enter global configuration mode on Switch 1.                                                                                                          |
| Step 2  | <b>interface fa0/1</b>                  | Enter interface configuration mode, and define Fa0/1 as the interface to be configured as a trunk.                                                    |
| Step 3  | <b>switchport mode trunk</b>            | Configure the port as a trunk port.                                                                                                                   |
| Step 4  | <b>end</b>                              | Return to global configuration mode.                                                                                                                  |
| Step 5  |                                         | Repeat Steps 2 through 4 on Switch 1 interface Fa0/2.                                                                                                 |
| Step 6  | <b>show running-config</b>              | Verify your entries.<br><br>In the display, make sure that interface Fa0/1 and Fa0/2 are configured as trunk ports.                                   |
| Step 7  | <b>show vlan</b>                        | When the trunk links come up, Switch 1 receives the VTP information from the other switches. Verify that Switch 1 has learned the VLAN configuration. |
| Step 8  | <b>configure terminal</b>               | Enter global configuration mode.                                                                                                                      |
| Step 9  | <b>interface fa0/1</b>                  | Enter interface configuration mode, and define Fa0/1 as the interface to set the STP cost.                                                            |
| Step 10 | <b>spanning-tree vlan 2 3 4 cost 30</b> | Set the spanning-tree path cost to 30 for VLANs 2, 3, and 4.                                                                                          |
| Step 11 | <b>end</b>                              | Return to global configuration mode.                                                                                                                  |
| Step 12 |                                         | Repeat Steps 9 through 11 on Switch 1 interface Fa0/2, and set the spanning-tree path cost to 30 for VLANs 8, 9, and 10.                              |

|         | Command                    | Purpose                                                                                                                 |
|---------|----------------------------|-------------------------------------------------------------------------------------------------------------------------|
| Step 13 | <b>exit</b>                | Return to privileged EXEC mode.                                                                                         |
| Step 14 | <b>show running-config</b> | Verify your entries.<br><br>In the display, verify that the path costs are set correctly for interface Fa0/1 and Fa0/2. |

The [“Finding More Information About IOS Commands”](#) section on page 4-1 contains the path to the complete IOS documentation set.





# Creating Performance Graphs and Link Reports

---

You can use the Cluster Management Suite to display real-time graphs that help you analyze traffic patterns and identify problems with individual links. You can also create a link report for each link in the cluster. The link report contains information about the two ports in the link, their configuration, and the devices that are connected to them. This chapter describes how to generate these graphs and reports and how to understand the information they contain.

## Displaying Link Graphs

To display a link graph, one end of the link must be connected to a port on a cluster member that is a Catalyst 2950, 2900 XL, and 3500 XL switch. The Simple Network Management Program (SNMP) must be enabled to generate graphs.

To display a link graph in Cluster Builder or Cluster View, right-click a link, and select **Link Graph** from the pop-up menu. To display a link graph in Cluster Manager, right-click a port that has a green status LED, and select **Link Graph** from the pop-up menu.

The graph runs as a separate browser session and can run in the background without interrupting the original session. The host name of the switch is displayed in the browser window title bar, and the link port number is displayed above the graph.

When the graph window is displayed ([Figure 6-1](#)), use the drop-down list in the upper-right corner to select the data you want to present.

Select one of the following graphs from the drop-down list:

- Percent utilization ([Figure 6-1](#))
- Total number of bytes sent and received
- Packets sent and received, including broadcast and multicast packets
- Total errors, including error packets and dropped packets

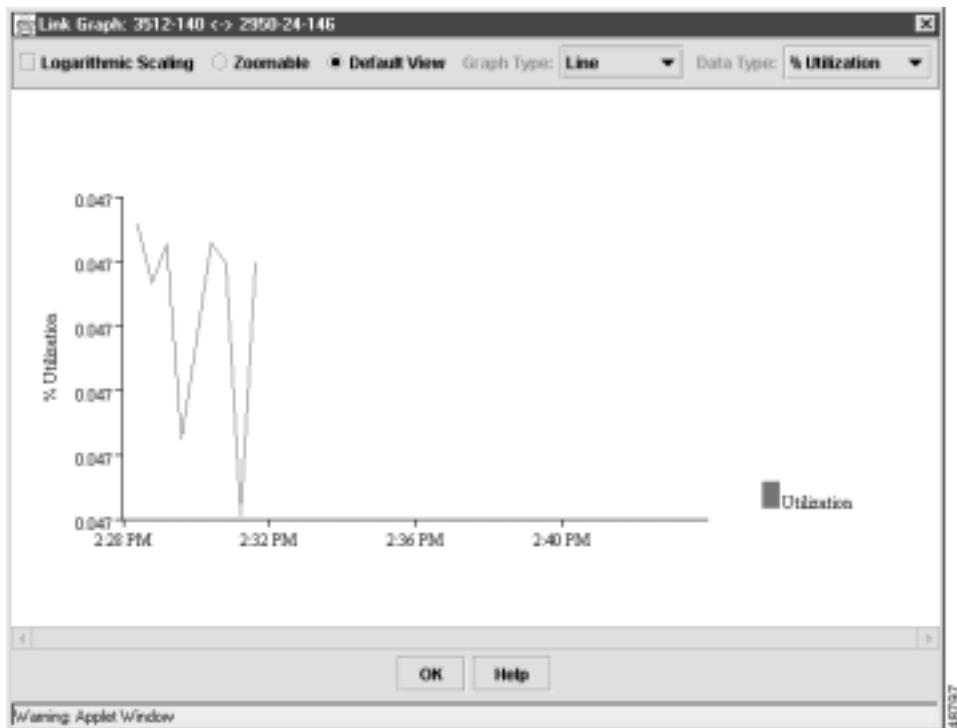
## Displaying the Percent Utilization

The graph shown in [Figure 6-1](#) displays the percentage of the maximum bandwidth in use by the port displayed on the graph.

## Displaying the Bandwidth Utilization Graph

On Catalyst 2950, 2900 XL, and 3500 XL switches, you can generate a graph of the switch bandwidth by selecting **Bandwidth Graph** from the device pop-up menu in Cluster Manager. The graph is an estimate of the traffic flowing through the switch.

**Figure 6-1** Link Graph (Percent Utilization)

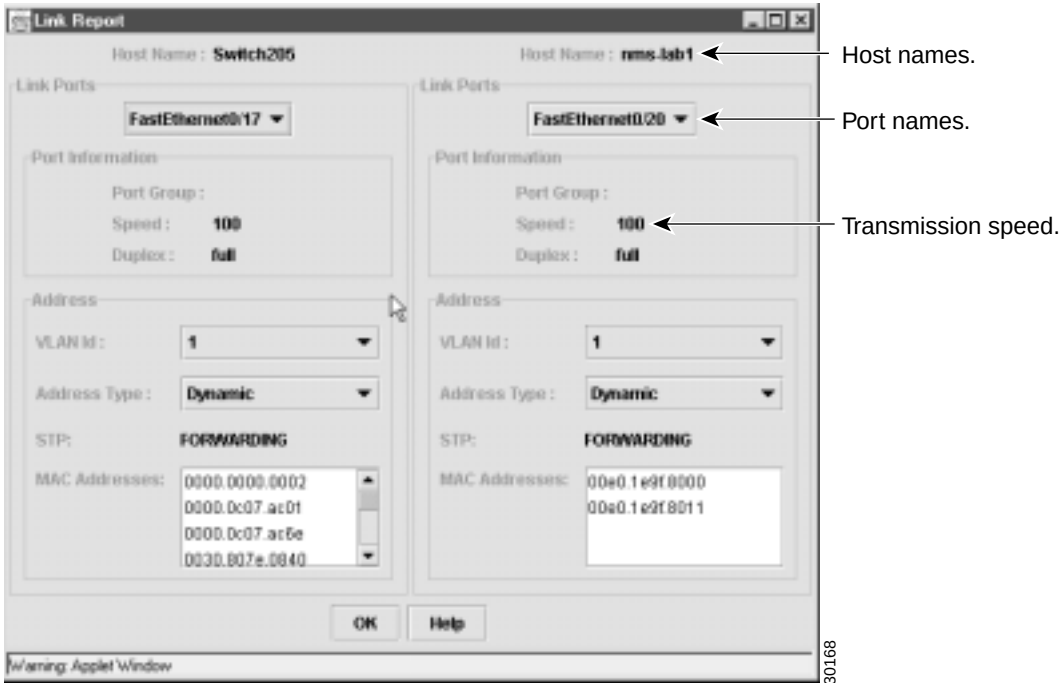


## Displaying the Link Report

Figure 6-2 shows the link report you can display by right-clicking on a link in Cluster Builder or Cluster View and selecting **Link Report** from the pop-up menu. The information on this report can be generated for any Catalyst 2900 XL, 2950, or 3500 XL switch.

■ Displaying the Link Report

Figure 6-2 Link Report







# Troubleshooting

---

This chapter describes how to identify and resolve software problems related to the IOS software. Depending on the nature of the problem, you can use the command-line interface (CLI) or Cluster Manager Suite (CMS) to identify and solve problems.

This chapter describes how to perform the following tasks:

- Identify an autonegotiation mismatch
- Recover from corrupted software
- Recover from a lost or forgotten password
- Recover from a failed command switch
- Maintain connectivity with cluster members

## Autonegotiation Mismatches

The IEEE 802.3u autonegotiation protocol manages the switch settings for speed (10 Mbps or 100 Mbps) and duplex (half or full). There are situations when this protocol can incorrectly align these settings, reducing performance. A mismatch occurs under these circumstances:

- A manually-set speed or duplex parameter is different from the manually set speed or duplex parameter on the connected port.
- A port is in autonegotiate and the connected port is set to full duplex with no autonegotiation.

To maximize switch performance and ensure a link, follow one of these guidelines when changing the settings for duplex and speed:

- Let both ports autonegotiate both speed and duplex.
- Manually set the speed and duplex parameters for the ports on both ends of the connection.

**Note**

If a remote Fast Ethernet device does not autonegotiate, configure the duplex settings on the two ports to match. The speed parameter can adjust itself even if the connected port does not autonegotiate. To connect to a remote Gigabit Ethernet device that does not autonegotiate, disable autonegotiation on the local device, and set the duplex and flow control parameters to be compatible with the remote device.

# Troubleshooting CMS Sessions

Table 7-1 lists problems commonly encountered when using CMS:

**Table 7-1 Common CMS Session Problems**

| Problem                                                                                                                         | Suggested Solution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A blank screen appears when you click <b>Cluster Management Suite</b> or <b>Visual Switch Manager</b> from the CMS access page. | <p>A missing Java plug-in or incorrect settings could cause this problem.</p> <ul style="list-style-type: none"> <li>CMS requires a Java plug-in order to function correctly. For instructions on downloading and installing the plug-ins refer to the <i>Release Notes for the Catalyst 2950 Cisco IOS Release 12.0(5)WC(1)</i>.</li> </ul> <p><b>Note</b> If your PC is connected to the Internet when you attempt to access CMS, the browser notifies you that the Java plug-in is required if the Java plug-in is not installed. This notification does not occur if your PC is directly connected to the switch and has no internet connection.</p> <ul style="list-style-type: none"> <li>If the plug-in is installed but the Java applet does not initialize, do the following: <ul style="list-style-type: none"> <li>Select <b>Start &gt; Programs &gt; Java Plug-in Control Panel</b>. In the <b>Proxies</b> tab, verify that <b>Use browser settings</b> is checked and that no proxies are enabled.</li> <li>Make sure that the HTTP port number is 80. CMS only works with port 80, which is the default HTTP port number.</li> <li>Make sure the port that connects the PC to the switch belongs to the same VLAN as the management VLAN. For more information about management VLANs, see the <a href="#">“Changing the Management VLAN for a Cluster”</a> section on page 3-35.</li> </ul> </li> </ul> |
| The <b>Applet notinited</b> message appears at the bottom of the browser window.                                                | You might not have enough disk space. Each time you start CMS, Java Plug-in 1.2.2 saves a copy of all the jar files to the disk. Delete the jar files from the location where the browser keeps the temporary files on your computer.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

**Table 7-1 Common CMS Session Problems (continued)**

| Problem                                                                                                                                                                                | Suggested Solution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| In an Internet Explorer browser session, you receive a message stating that the CMS page might not display correctly because your security settings prohibit running ActiveX controls. | <p>A high security level prohibits ActiveX controls (which Internet Explorer uses to launch the Java plug-in) from running. Do the following:</p> <ol style="list-style-type: none"> <li>1. Start Internet Explorer.</li> <li>2. From the menu bar, select <b>Tools &gt; Internet Options</b>.</li> <li>3. Click the <b>Security</b> tab.</li> <li>4. Click the indicated <b>Zone</b>.</li> <li>5. Move the <b>Security Level for this Zone</b> slider from <b>High</b> to <b>Medium</b> (the default).</li> <li>6. Click <b>Custom Level...</b> and verify that the following ActiveX controls and plug-ins are set to either <b>Prompt</b> or <b>Enable</b>: <ul style="list-style-type: none"> <li>• Download signed ActiveX controls</li> <li>• Download unsigned ActiveX controls as safe</li> <li>• Initialize and script ActiveX controls not marked</li> <li>• Run ActiveX controls and plug-ins</li> </ul> </li> </ol> |

For further debugging information, you can use the Java plug-ins Java console to display the current status and actions of CMS. To display the Java console, select **Start > Programs > Java Plug-in Control Panel**, and select **Show Java Console**.

## Recovery Procedures

The recovery procedures in this section require that you have physical access to the switch. Recovery procedures include the following topics:

- Recovering from corrupted software
- Recovering from a lost or forgotten password
- Recovering from a command-switch failure

## Recovering from Corrupted Software

Switch software can be corrupted during an upgrade, by downloading the wrong file to the switch, and by deleting the image file. In all these cases, the switch does not pass the power-on self-test (POST), and there is no connectivity.

The following procedure uses the XMODEM Protocol to recover from a corrupt or wrong image file. There are many software packages that support the XMODEM protocol, and this procedure is largely dependent on the emulation software you are using.

---

**Step 1** Connect a PC with terminal-emulation software supporting the XMODEM Protocol to the switch console port.

**Step 2** Set the line speed on the emulation software to 9600 baud.

**Step 3** Unplug the switch power cord.

**Step 4** Reconnect the power cord to the switch.

The software image does not load. The switch starts in boot loader mode, which is indicated by the `switch:` prompt

**Step 5** Use the boot loader to enter commands, and start the transfer.

```
switch: copy xmodem: flash:image_filename.bin
```

**Step 6** When the XMODEM request appears, use the appropriate command on the terminal-emulation software to start the transfer and to copy the software image into Flash memory.

---

## Recovering from a Lost or Forgotten Password

Follow the steps in this procedure if you have forgotten or lost the switch password.

- Step 1** Connect a terminal or PC with terminal emulation software to the console port. For more information, refer to the switch installation guide.



**Note** You can configure your switch for Telnet by following the procedure in [“Configuring the Switch for Telnet” section on page 2-32](#).

- Step 2** Set the line speed on the emulation software to 9600 baud.
- Step 3** Unplug the switch power cord.
- Step 4** Press in the **Mode** button, and at the same time reconnect the power cord to the switch.

You can release the **Mode** button a second or two after the LED above port 1X goes off. Several lines of information about the software appear, as do instructions:

The system has been interrupted prior to initializing the flash file system. The following commands will initialize the flash file system, and finish loading the operating system software:

```
flash_init
boot
```

- Step 5** Initialize the Flash file system:
- ```
switch: flash_init
```
- Step 6** If you had set the console port speed to anything other than 9600, it has been reset to that particular speed. Change the emulation software line speed to match that of the switch console port.

**Step 7** Display the contents of Flash memory as in this example:

switch: **dir flash:**

The switch file system is displayed:

```
Directory of flash:/
 3  drwx      10176   Mar 01 2001 00:04:34  html
 6  -rwx       2343   Mar 01 2001 03:18:16  config.text
171 -rwx     1667997   Mar 01 2001 00:02:39  c2950-c3h2s-mz.120-5.WC.1.bin
 7  -rwx       3060   Mar 01 2001 00:14:20  vlan.dat
172 -rwx        100   Mar 01 2001 00:02:54  env_vars

7741440 bytes total (4788224 bytes free)
```

**Step 8** Rename the configuration file to config.text.old.

This file contains the password definition.

switch: **rename flash:config.text flash:config.text.old**

**Step 9** Boot the system:

switch: **boot**

You are prompted to start the setup program. Enter **N** at the prompt:

Continue with the configuration dialog? [yes/no]: **N**

**Step 10** At the switch prompt, change to privileged EXEC mode:

switch> **enable**

**Step 11** Rename the configuration file to its original name:

switch# **rename flash:config.text.old flash:config.text**

**Step 12** Copy the configuration file into memory:

switch# **copy flash:config.text system:running-config**

Source filename [config.text]?

Destination filename [running-config]?

Press **Return** in response to the confirmation prompts.

The configuration file is now reloaded, and you can use the following normal commands to change the password.

**Step 13** Enter global configuration mode:

switch# **config terminal**

**Step 14** Change the password:

```
switch(config)# enable secret <password>  
or
```

```
switch(config)# enable password <password>
```

**Step 15** Return to privileged EXEC mode:

```
switch(config)# exit  
switch#
```

**Step 16** Write the running configuration to the startup configuration file:

```
switch# copy running-config startup-config
```

The new password is now included in the startup configuration.

---

## Recovering from a Command Switch Failure

This section describes how to recover from a failed command switch. If you are running IOS Release 12.0(5)WC(1), you can configure a redundant command switch group by using the Hot Standby Router Protocol (HSRP). For more information, see the [“Building a Redundant Cluster” section on page 3-17](#).



### Note

---

HSRP is the preferred method for supplying redundancy to a cluster.

---

If you have not configured a standby command switch, and your command switch loses power or fails in some other way, management contact with the member switches is lost, and a new command switch must be installed. However, connectivity between switches that are still connected is not affected, and the member switches forward packets as usual. You can manage the members as standalone switches through the console port or, if they have IP addresses, through the other management interfaces.



You can prepare for a command switch failure by assigning an IP address to a member switch or another switch that is command-capable, making a note of the command-switch password, and cabling your cluster to provide redundant connectivity between the member switches and the replacement command switch. This section describes two solutions for replacing a failed command switch:

- Replacing a failed command switch with a cluster member
- Replacing a failed command switch with another switch

For information on command-capable switches, see the [“Supported Hardware” section on page 1-3](#).

## Replacing a Failed Command Switch with a Cluster Member

Follow these steps to replace a failed command switch with a command-capable member of the same cluster:

- 
- Step 1** Disconnect the command switch from the member switches and physically remove it from the cluster.
- Step 2** Insert the member switch in place of the failed command switch, and duplicate its connections to the cluster members.
- Step 3** Start a CLI session on the new command switch.
- You can access the CLI by using the console port or, if an IP address has been assigned to the switch, by using Telnet. For details about using the console port, refer to the switch installation guide.
- Step 4** At the switch prompt, change to privileged EXEC mode:
- ```
Switch> enable
Switch#
```
- Step 5** Enter the password of the *failed command switch*.
- Step 6** From privileged EXEC mode, enter global configuration mode.
- ```
Switch# config terminal
```
- Enter configuration commands, one per line. End with CNTL/Z.
- Step 7** From global configuration mode, remove the member switch from the cluster.
- ```
Switch(config)# no cluster commander-address
```

- Step 8** Return to privileged EXEC mode.
- ```
Switch(config)# exit
Switch#
```
- Step 9** Use the setup program to configure the switch IP information.
- This program prompts you for an IP address, subnet mask, default gateway, and password. From privileged EXEC mode, enter **setup**, and press **Return**.
- ```
Switch# setup

--- System Configuration Dialog ---

At any point you may enter a question mark '?' for help.
Use Ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Continue with configuration dialog? [yes/no]:
```
- Step 10** Enter **Y** at the first prompt:
- ```
Continue with configuration dialog? [yes/no]: y
```
- If this prompt does not appear, enter **enable**, and press **Return**. Enter **setup**, and press **Return** to start the setup program.
- Step 11** Enter the switch IP address, and press **Return**:
- ```
Enter IP address: ip_address
```
- Step 12** Enter the subnet mask (IP netmask) address, and press **Return**:
- ```
Enter IP netmask: ip_netmask
```
- Step 13** Enter **Y** to enter a default gateway (router) address:
- ```
Would you like to enter a default gateway address? [yes]: y
```
- Step 14** Enter the IP address of the default gateway (router), and press **Return**:
- ```
Enter router IP address: IP_address
```
- Step 15** Enter a host name, and press **Return**:
- ```
Enter host name: host_name
```
- Step 16** Enter the password of the failed command switch again, and press **Return**:
- ```
Enter enable secret password: secret_password
```
- Step 17** Enter a Telnet password, and press **Return**:
- ```
Would you like to configure a telnet password? [yes]: y
Enter telnet password: password
```

The initial configuration displays:

The following configuration command script was created:

```
ip subnet-zero
interface VLAN1
ip address IP_address IP_netmask
ip default-gateway IP_address
hostname host_name
enable secret 5 $1$yDsa$/YLihJcV8e/H0Dagkw1Ff0
line vty 0 15
password password
snmp community private rw
snmp community public ro
!
end
```

Use this configuration? [yes/no]:

- Step 18** Verify that the addresses are correct.
- Step 19** Enter **Y**, and press **Return** if the displayed information is correct.  
If this information is not correct, enter **N**, press **Return**, and begin again at Step 9.
- Step 20** Start your browser, and enter the IP address you just entered for the switch.
- Step 21** Display the VSM Home page for the switch, and select **Enabled** from the Command Switch drop-down list.
- Step 22** Click **Cluster Management**, and display Cluster Builder.  
CMS prompts you to add candidate switches. The password of the failed command switch is still valid for the cluster, and you should enter it when candidate switches are proposed for cluster membership.



**Note** You can also add switches to the cluster by using the CLI. For the complete instructions, see the [“Adding and Removing Member Switches”](#) section on page 3-12.

## Replacing a Failed Command Switch with Another Switch

Follow these steps when you are replacing a failed command switch with a switch that is command capable but not part of the cluster:

- 
- Step 1** Insert the new switch in place of the failed command switch, and duplicate its connections to the cluster members.
- Step 2** Start a CLI session on the new command switch.
- You can access the CLI by using the console port or, if an IP address has been assigned to the switch, by using Telnet. For details about using the console port, refer to the switch installation guide.
- Step 3** At the switch prompt, change to privileged EXEC mode:
- ```
Switch> enable
Switch#
```
- Step 4** Enter the password of the *failed command switch*.
- Step 5** Use the setup program to configure the switch IP information.
- This program prompts you for an IP address, subnet mask, default gateway, and password. From privileged EXEC mode, enter **setup**, and press **Return**.
- ```
Switch# setup
      --- System Configuration Dialog ---

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Continue with configuration dialog? [yes/no]:
```
- Step 6** Enter **Y** at the first prompt:
- ```
Continue with configuration dialog? [yes/no]: y
```
- If this prompt does not appear, enter **enable**, and press **Return**. Enter **setup**, and press **Return** to start the setup program.
- Step 7** Enter the switch IP address, and press **Return**:
- ```
Enter IP address: ip_address
```
- Step 8** Enter the subnet mask (IP netmask) address, and press **Return**:
- ```
Enter IP netmask: ip_netmask
```
- Step 9** Enter **Y** to enter a default gateway (router) address:
- ```
Would you like to enter a default gateway address? [yes]: y
```

**Step 10** Enter the IP address of the default gateway (router), and press **Return**:

Enter router IP address: *IP\_address*

**Step 11** Enter a host name, and press **Return**:

Enter host name: *host\_name*

**Step 12** Enter the password of the failed command switch again, and press **Return**:

Enter enable secret password: *secret\_password*

**Step 13** Enter a Telnet password, and press **Return**:

Would you like to configure a telnet password? [yes]: **y**

Enter telnet password: *password*

The initial configuration displays:

The following configuration command script was created:

```
ip subnet-zero
interface VLAN1
ip address IP_address IP_netmask
ip default-gateway IP_address
hostname host_name
enable secret 5 $1$yDsa$/YLhJcV8e/H0Dagkw1Ff0
line vty 0 15
password password
snmp community private rw
snmp community public ro
!
end
```

Use this configuration? [yes/no]:

**Step 14** Verify that the addresses are correct.

**Step 15** Enter **Y**, and press **Return** if the displayed information is correct.

If this information is not correct, enter **N**, press **Return**, and begin again at Step 5.

**Step 16** Start your browser, and enter the IP address you just entered for the switch.

**Step 17** Click **Cluster Manager Suite or Visual Switch Manager**, and display Cluster Builder.

It prompts you to add the candidate switches. The password of the failed command switch is still valid for the cluster. Enter it when candidate switches are proposed for cluster membership, and click **OK**.

**Note**

You can also add switches to the cluster by using the CLI. For the complete instructions, see the [“Adding and Removing Member Switches”](#) section on page 3-12.

## Recovering from Lost Member Connectivity

Some configurations can prevent the command switch from maintaining contact with member switches. If you are unable to maintain management contact with a member, and the member switch is forwarding packets normally, check for the following port-configuration conflicts:

- Member switches cannot connect to the command switch through a port that is defined as a network port. For information on the network port feature, see the [“Managing the System Date and Time”](#) section on page 4-22.
- Member switches must connect to the command switch through a port that belongs to the same management VLAN. For more information, see the [“Understanding Management VLAN Changes”](#) section on page 3-4.
- Member switches connected to the command switch through a secured port can lose connectivity if the port is disabled due to a security violation. Secured ports are described in the [“Enabling Port Security”](#) section on page 4-58.



# System Error Messages

---

This chapter describes the IOS system error messages for the Catalyst 2950 switches. The system software sends these error messages to the console (and, optionally, to a logging server on another system) during operation. Not all system error messages indicate problems with your system. Some messages are purely informational, while others might help diagnose problems with communications lines, internal hardware, or the system software.

This chapter contains the following sections:

- [How to Read System Error Messages, page A-1](#)
- [Error Message Traceback Reports, page A-4](#)

## How to Read System Error Messages

System error messages begin with a percent sign (%) and are structured as follows:

%FACILITY-SUBFACILITY-SEVERITY-MNEMONIC: Message-text

- FACILITY is a code consisting of two or more uppercase letters that indicate the facility to which the message refers. A facility can be a hardware device, a protocol, or a module of the system software. [Table A-1](#) lists the system facility codes.

**Table A-1 Facility Codes**

| Code          | Facility                    |
|---------------|-----------------------------|
| CMP           | Cluster Membership Protocol |
| ENVIRONMENT   | Environment                 |
| LINK          | Link                        |
| PORT SECURITY | Port Security               |
| RTD           | Runtime Diagnostic          |
| STORM CONTROL | Storm Control               |

- SEVERITY is a single-digit code from 0 to 7 that reflects the severity of the condition. The lower the number, the more serious the situation. [Table A-2](#) lists the message severity levels.
- MNEMONIC is a code that uniquely identifies the error message.

**Table A-2 Message Severity Levels**

| Severity Level    | Description                                 |
|-------------------|---------------------------------------------|
| 0 – emergency     | System is unusable.                         |
| 1 – alert         | Immediate action required.                  |
| 2 – critical      | Critical condition.                         |
| 3 – error         | Error condition.                            |
| 4 – warning       | Warning condition.                          |
| 5 – notification  | Normal but significant condition.           |
| 6 – informational | Informational message only.                 |
| 7 – debugging     | Message that appears during debugging only. |

- Message-text is a text string describing the condition. This portion of the message sometimes contains detailed information about the event, including terminal port numbers, network addresses, or addresses that correspond to locations in the system memory address space. Because the information in these variable fields changes from message to message, it is represented here



by short strings enclosed in square brackets ([ ]). A decimal number, for example, is represented as [dec]. [Table A-3](#) lists the variable fields in messages.

**Table A-3 Representation of Variable Fields in Messages**

| Representation | Type of Information |
|----------------|---------------------|
| [dec]          | Decimal             |
| [char]         | Single character    |
| [chars]        | Character string    |
| [hex]          | Hexadecimal integer |
| [inet]         | Internet address    |

The following is a sample system error message:

%LINK-2-BADVCALL: Interface [chars], undefined entry point

Some error messages also indicate the card and slot reporting the error. These error messages begin with a percent sign (%) and are structured as follows:

%CARD-SEVERITY-MSG:SLOT %FACILITY-SEVERITY-MNEMONIC:  
Message-text

CARD is a code that describes the type of card reporting the error.

MSG is a mnemonic that indicates this is a message. It is always shown as MSG.

SLOT indicates the slot number of the card reporting the error. It is shown as SLOT followed by a number. (For example, SLOT5.)

# Error Message Traceback Reports

Some messages describe internal errors and contain traceback information. This information is very important and should be included when you report a problem to your technical support representative.

The following sample message includes traceback information:

-Process= "Exec", level= 0, pid= 17

-Traceback= 1A82 1AB4 6378 A072 1054 1860

## Error Message and Recovery Procedures

This section lists the switch system messages by facility. Within each facility, the messages are listed by severity levels 0 to 7: 0 is the highest severity level, and 7 is the lowest severity level. Each message is followed by an explanation and a recommended action.

### CMP Messages

This section contains the Cluster Membership Protocol (CMP) error messages.

**CMP-5-ADD:** The Device is added to the cluster (Cluster Name:[chars], CMDR IP Address [inet])

**Explanation** The message indicates the device is added to the cluster: [chars] is the cluster name, and [inet] is the internet address of the command switch.

**Action** No action is required.

CMP-5-MEMBER\_CONFIG\_UPDATE: Received member configuration from member [dec]

**Explanation** This message indicates that the command switch received a member configuration: [dec] is the member number.

**Action** No action is required.

CMP-5-REMOVE The Device is removed from the cluster (Cluster Name:[chars])

**Explanation** The message indicates the device is removed from the cluster: [chars] is the cluster name.

**Action** No action is required.

## Environment Messages

This section contains the Environment error messages.

### ENVIRONMENT-2-FAN\_FAULT

**Explanation** This message indicates that an internal fan fault is detected.

**Action** Either check the switch itself or use the **show env** command to determine if a fan on the switch has failed. The Catalyst 2950 switch can operate normally with one failed fan. Replace the switch at your convenience.

### ENVIRONMENT-2-OVER\_TEMP

**Explanation** This message indicates that an overtemperature condition is detected.

**Action** Use the **show env** command to check if an overtemperature condition exists. If it does:

- Place the switch in an environment that is within 32 to 113°F (0 to 45°C).
- Make sure fan intake and exhaust areas are clear.

- If a multiple-fan failure is causing the switch to overheat, replace the switch.

## Link Messages

This section contains the Link error message.

LINK-4-ERROR [chars] is experiencing errors.

**Explanation** This messages indicates that excessive errors have occurred on this interface: [char] is the interface.

**Action** Check for duplex mismatches between both ends of the link.

## Port Security Messages

This section contains the Port Security error message.

PORT\_SECURITY-2-SECURITYREJECT

**Explanation** This message indicates that a packet with an unexpected MAC source address is received on a secure port.

**Action** Remove the station with the unexpected MAC address from the secure port, or add the MAC address to the secure address table of the secure port.

## RTD Messages

This section contains the Runtime Diagnostic (RTD) error messages.

RTD-1-ADDR\_FLAP [chars] relearning [dec] addrs per min

**Explanation** Normally, MAC addresses are learned once on a port. Occasionally, when a switched network reconfigures, due to either manual or STP reconfiguration, addresses learned on one port are relearned on a different

port. However, if there is a port anywhere in the switched domain that is looped back to itself, addresses will jump back and forth between the real port and the port that is in the path to the looped back port. In this message, [chars] is the interface, and [dec] is the number of addresses being learnt.

**Action** Determine the real path (port) to the MAC address. Use **debug ethernet-controller addr** to see the alternate path-port on which the address is being learned. Go to the switch attached to that port. Note that **show cdp neighbors** is useful in determining the next switch. Repeat this procedure until the port is found that is receiving what it is transmitting, and remove that port from the network.

RTD-1-LINK\_FLAP [chars] link down/up [dec] times per min

**Explanation** This message indicates that an excessive number of link down-up events has been noticed on this interface: [chars] is the interface, and [dec] is the number of times the link goes up and down. This might be the result of reconfiguring the port, or it might indicate a faulty device at the other end of the connection.

**Action** If someone is reconfiguring the interface or device at the other side of the interface, ignore this message. However, if no one is manipulating the interface or device at the other end of the interface, it is likely that the Ethernet transceiver at one end of the link is faulty and should be replaced.

## Storm Control Messages

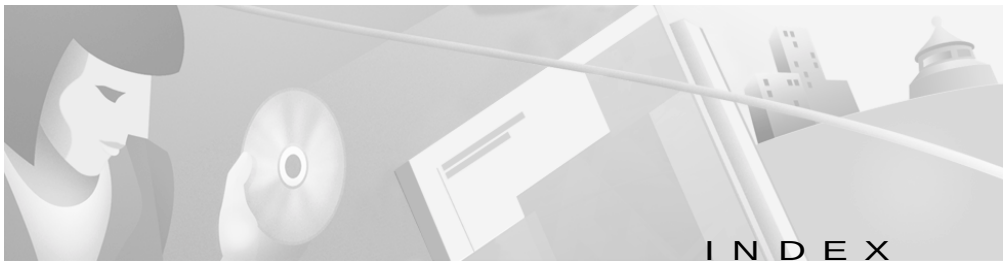
This section contains the Storm Control error message.

STORM\_CONTROL - 2 - SHUTDOWN

**Explanation** This messages indicates that excessive traffic has been detected on a port that has been configured to be shut down if a storm event is detected.

**Action** Once the source of the packet storm has been fixed, re-enable the port by using port-configuration commands.





## INDEX

---

## A

### AAA

- configuring [4-107](#)
- managing [4-101](#)

aaa accounting command [4-106](#)

aaa authorization command [4-105](#)

aaa authorization exec tacacs+ local  
command [4-106](#)

aaa new-model command [4-104, 4-107](#)

### abbreviations

- char, variable field [A-3](#)
- chars, variable field [A-3](#)
- dec, variable field [A-3](#)
- hex, variable field [A-3](#)
- inet, variable field [A-3](#)

### accessing

- CMS [2-2](#)
- command modes [2-25](#)
- member switches [5-6, 5-28](#)
- MIB files [2-35](#)
- MIB objects [2-34, 2-35](#)
- MIB variables [2-35](#)

accounting in TACACS+ [4-102](#)

### adding

Ethernet VLAN to database [5-25](#)

member switches to standby group [3-24](#)

secure addresses [4-52, 4-54](#)

static addresses [4-55, 4-57](#)

switches to cluster [3-12](#)

### address

count, secure [4-60](#)

resolution [4-47](#)

security violations [4-59](#)

see also addresses

### addresses

#### dynamic

- accelerated aging [4-83](#)
- aging time [4-50, 4-51](#)
- default aging [4-83](#)
- described [4-49](#)
- removing [4-52](#)

### MAC

- adding secure [4-52](#)
- aging time [4-50](#)
- discovering [4-47, 4-50](#)
- tables, managing [4-49](#)

- secure
  - adding 4-52, 4-54
  - described 4-49, 4-52
  - removing 4-55
- static
  - adding 4-55, 4-57
  - configuring (EtherChannel) 4-57
  - described 4-49, 4-55
  - removing 4-58
- Address Management window 4-50
- Address Resolution Protocol (ARP)
  - see ARP table
- address table
  - aging time, configuring 4-51
  - dynamic addresses, removing 4-52
  - MAC 4-49
  - secure addresses
    - adding 4-54
    - removing 4-55
  - static addresses
    - adding 4-57
    - removing 4-58
- administrative information, displaying 3-33
- advertisements, VTP 5-9
- aggregation
  - enterprise workgroup 1-6
  - small to medium business workgroup 1-7
- aging, accelerating 4-83
- aging time, changing address 4-50, 4-51

- alarms group, in RMON 2-38
- allowed-VLAN list 5-34
- AppleTalk Remote Access (ARA) 4-105
- Apply button 2-4
- ARP table
  - address resolution 4-47
  - illustrated 4-48
  - managing 4-47
- authentication, enabling NTP 4-26
- authentication in TACACS+ 4-102
- authorization in TACACS+ 4-102
- autonegotiation
  - connecting to devices without 3-41
  - mismatches 7-1

---

## B

- bandwidth, graphing 2-19
- BPDU message interval 4-92
- broadcast client mode, configuring 4-26
- broadcast messages, configuring for 4-26
- broadcast storm control
  - disabling 4-21
  - enabling 4-18, 4-20
- broadcast traffic and protected ports 4-101
- buttons, CMS window 2-4
- bytes, graphing 6-2



---

## C

C2900/C3500 traps [3-63, 4-45](#)

cabling, redundant [3-17](#)

Cancel button [2-4](#)

candidates

- adding [3-12](#)

- automatically discovering [3-6](#)

- changing management VLAN for [3-37](#)

- displaying all [3-14](#)

- requirements [3-3](#)

- suggested [3-6](#)

- why not added [3-13](#)

Caution described [xvii](#)

caveats

- password and privilege level [3-11](#)

CDP

- configuring [4-62, 4-63](#)

- disabling for routing device [4-67, 4-68](#)

- discovering candidates with [3-6](#)

Cisco Discovery Protocol

- see CDP

Cisco Systems access page [3-29](#)

CiscoWorks, as an example of CMS [2-36](#)

Class of Service

- see CoS

CLI

- accessing [1-5](#)

- command modes [2-25](#)

- error messages [2-31](#)

- managing cluster members with [2-29](#)

- using [2-24](#)

client mode, VTP [5-8](#)

Cluster Builder

- changing the polling interval [3-31](#)

- device and link icons [2-7](#)

- illustrated [3-13](#)

- interface [2-5](#)

- label meanings [2-9](#)

- menu options [2-7](#)

- overview [1-5](#)

- pop-up menus [2-11, 2-12](#)

- saving configuration changes [3-33](#)

- starting [2-20](#)

- toolbar icons [2-6](#)

- using [2-9](#)

Cluster management described [3-1](#)

Cluster Management Suite

- see CMS

Cluster Management Suite (CMS) [2-35](#)

Cluster Manager

- menu options [2-15](#)

- overview [1-4](#)

- pop-up menus [2-17, 2-18](#)

- toolbar icons [2-19](#)

- using [2-14](#)

- clusters
  - accessing [3-5](#)
  - adding switches to [3-12, 3-14](#)
  - configuring [3-5, 3-8](#)
  - creating [2-9](#)
  - creating performance graphs [6-1](#)
  - described [3-1, 5-4](#)
  - disqualification code [3-13](#)
  - host name changes [3-10](#)
  - inventory, displaying [3-33](#)
  - management tasks [3-27](#)
  - management VLAN, changing [3-35](#)
  - managing [2-29, 2-37, 3-1](#)
  - password changes [3-11](#)
  - planning [3-2](#)
  - redundancy [3-2, 3-17](#)
  - removing switches from [3-12, 3-14](#)
  - settings, configuring initial [3-30](#)
  - see also candidates, command switch,  
member switches, standby groups
- cluster setup command [3-14](#)
- cluster tree [2-19](#)
- Cluster View
  - device and link icons [2-7](#)
  - device menu options [2-14](#)
  - displaying [3-13](#)
  - interface [2-5](#)
  - menu options [2-7](#)
  - overview [1-5](#)
  - toolbar icons [2-6](#)
  - using [2-13](#)
- CMS [2-35](#)
  - accessing [2-2, 3-28](#)
  - overview [1-4](#)
  - privilege level [2-28](#)
  - using [2-3](#)
  - windows, using [2-3](#)
- colors
  - devices in CMS [2-9](#)
- command-line error messages [2-31](#)
- command-line interface
  - see CLI
- command modes [2-25, 2-26](#)
- commands
  - ? [2-30](#)
  - aaa accounting [4-106](#)
  - aaa authorization [4-105](#)
  - aaa authorization exec tacacs+ local [4-106](#)
  - abbreviating [2-30](#)
  - cluster setup [3-14](#)
  - copy running-config startup-config [2-34](#)
  - default [2-31](#)
  - dir flash [2-33](#)
  - help [2-30](#)
  - list of available [2-27, 2-30](#)
  - name [3-22](#)
  - no [2-31](#)
  - preempt [3-22](#)
  - rcommand [2-29](#)

- redisplaying [2-30](#)
- redundancy-enable [3-22](#)
- resetting to defaults [2-31](#)
- show cluster candidates [3-14](#)
- show cluster members [2-29, 3-14](#)
- spanning-tree root guard [4-99](#)
- stp-list [4-80](#)
- undoing [2-31](#)
- command switch
  - and management [1-5](#)
  - and managing with SNMP [2-37](#)
  - configuration conflicts [7-14](#)
  - defined [1-3, 3-1](#)
  - enabling [3-5, 4-10](#)
  - privilege levels [2-29](#)
  - recovery
    - from failure [3-19, 7-8](#)
    - from failure without HSRP [3-19](#)
    - from lost member connectivity [7-14](#)
  - redundant (standby) [3-17](#)
  - removing from standby group [3-25](#)
  - replacing
    - with another switch [7-12](#)
    - with cluster member [7-9](#)
  - requirements [3-3](#)
  - standby [3-17, 3-18, 3-20](#)
  - see also candidates, member switches
- command variables, listing [2-30](#)
- community strings
  - added to new members [3-10](#)
  - configuring [3-10, 3-60, 4-42](#)
  - SNMP [2-37, 3-10](#)
- compatibility
  - cluster [3-2](#)
  - feature [4-2](#)
- config trap [3-63, 4-45](#)
- configuration
  - changes
    - saving [3-33](#)
  - conflicts, managing [4-2, 7-14](#)
  - default VLAN [5-21](#)
  - files, saving to an external server [2-33](#)
  - guidelines
    - port [3-41](#)
    - VLANs [5-20](#)
    - VTP [5-10](#)
    - VTP version [5-11](#)
  - saving to Flash memory [2-34](#)
  - VTP, default [5-12](#)
  - see also configuring
- configuring
  - 802.1p class of service [5-37](#)
  - AAA [4-107](#)
  - aging time [4-51](#)
  - broadcast messages [4-26](#)
  - broadcast storm control [4-19](#)
  - CDP [4-62, 4-63](#)
  - clusters [3-5, 3-8](#)

- cluster settings, initial [3-30](#)
- community strings [3-10, 3-60, 4-42](#)
- date and time [4-22](#)
- daylight saving time [4-23](#)
- DNS [4-39](#)
- duplex [3-38, 3-49](#)
- flooding controls [4-18](#)
- flow control [3-49](#)
- hello time [4-92](#)
- hops [4-64](#)
- HSRP groups [3-22](#)
- IP information [4-26](#)
- load sharing [5-45, 5-48](#)
- login authentication [4-104](#)
- management VLAN [3-37](#)
- multicast router port [4-79](#)
- native VLANs [5-36](#)
- NTP [4-24](#)
- passwords [2-27](#)
- Port Fast [3-38](#)
- ports [3-42](#)
  - multiple mixed [3-43](#)
  - protected port [4-100](#)
  - through Cluster Manager [2-17, 3-38](#)
  - through VSM [2-21](#)
- privilege levels [2-27](#)
- redundant clusters [3-17](#)
- RMON groups [2-38](#)
- SNMP [3-59, 4-41](#)
- speed [3-38, 3-41, 3-49](#)
- standalone switches [4-9](#)
- standby group [3-22](#)
- standby groups [3-19, 3-22](#)
- static addresses (EtherChannel) [4-57](#)
- STP [4-80](#)
  - path costs [5-48](#)
  - port priorities [5-45](#)
  - root guard [4-98, 4-99](#)
- switches
  - member [2-29](#)
  - overview [4-1](#)
  - standalone [4-9](#)
- TACACS+ [4-101](#)
- trap managers [3-63, 4-44](#)
- trunk port [5-31](#)
- trunks [5-30, 5-33](#)
- VLANs [5-1, 5-5, 5-20, 5-24](#)
- voice ports [4-108](#)
- VTP [5-10, 5-12](#)
  - VTP client mode [5-15](#)
  - VTP server mode [5-14](#)
  - VTP transparent mode [5-6, 5-16](#)
- configuring a multicast router port [4-76](#)
- conflicts
  - configuration [4-2, 7-14](#)
  - upgrade [3-55](#)
- consistency checks in VTP version 2 [5-10](#)
- conventions

- command [xvi](#)
- for examples [xvi](#)
- Note and Caution [xvii](#)
- text [xvi](#)
- copy running-config startup-config command [2-34](#)
- CoS [3-39](#)
  - configuring [5-37](#)
  - configuring priority queues [5-42](#)
  - defining [5-39](#)

---

## D

- database, VTP [5-19, 5-24](#)
- date, setting [4-22](#)
- daylight saving time [4-23](#)
- default configuration
  - VLANs [5-21](#)
  - VTP [5-12](#)
- defaults, resetting to [2-31](#)
- default settings, changing [4-3](#)
- deleting VLAN from database [5-27](#)
- deployment examples [1-6](#)
- destination-based forwarding [4-14](#)
- destination-based port groups [4-12, 4-57](#)
- device arrangement [3-32](#)
- device pop-up menu [2-18](#)
- DHCP [4-29](#)
  - configuring
    - DHCP server [4-32](#)
    - DNS [4-33](#)
    - example [4-37](#)
    - relay device [4-34](#)
    - TFTP server [4-33](#)
- dir flash command [2-33](#)
- disabling
  - broadcast storm control [4-21](#)
  - port security [4-62](#)
  - SNMP [4-42](#)
  - SNMP agent [3-60](#)
  - STP [4-83, 4-84](#)
  - Switch Port Analyzer (SPAN) [4-18](#)
  - trunking on a port [5-34](#)
  - trunk port [5-34](#)
  - VTP [5-16](#)
  - VTP version 2 [5-18](#)
- disqualification code [3-13](#)
- DNS
  - configuring [4-39](#)
  - described [4-39](#)
  - enabling [4-41](#)
- documentation, related [xvii](#)
- domain name
  - described [4-39](#)
  - specifying [4-39, 4-40, 5-10](#)
- Domain Name System server
  - see DNS
- domains for VLAN management [5-7](#)
- DTP [5-33](#)

## duplex

- configuration guidelines [3-41](#)
- configuring [3-49](#)

## dynamic addresses

- see addresses

## Dynamic Host Configuration Protocol

- see DHCP

Dynamic Trunk Protocol (DTP) [5-33](#)


---

**E**
egress port scheduling [5-38](#)eligible switches [3-20](#)

## enable password

- see passwords

## enable secret password

- see passwords

## enabling

- broadcast storm control [4-18, 4-20](#)
- command switch [3-5, 4-10](#)

DNS [4-41](#)HSRP [3-22](#)NTP authentication [4-26](#)Port Fast [4-95, 4-97](#)port security [4-58, 4-61](#)SNMP [4-42](#)SNMP agent [3-60](#)STP Port Fast [4-95, 4-97](#)Switch Port Analyzer (SPAN) [4-15, 4-17](#)traps [3-63](#)UplinkFast [4-87](#)VTP version 2 [5-17](#)encapsulation [5-37](#)enterprise workgroup aggregation [1-6](#)error messages [2-31](#)errors, graphing [6-2](#)

## EtherChannel port groups

- configuring static address for [4-57](#)
- creating [4-11, 4-15](#)

## Ethernet VLAN

- adding to database [5-25](#)
- defaults and ranges [5-21](#)
- modifying [5-26](#)

events group, in RMON [2-38](#)

## examples

- conventions for [xvi](#)
- deployment [1-6](#)

extended discovery [4-63](#)


---

**F**
facility codes [A-1](#)Fast EtherChannel port groups, creating [4-11](#)Fast Ethernet trunks [5-29](#)FDDI-Net VLAN defaults and ranges [5-22](#)FDDI VLAN defaults and ranges [5-21](#)

## features

- configuration conflicts between [2-25](#)

- default settings [4-2](#)

- incompatible [4-2](#)

- IOS [1-2](#)

Flash memory, files in [2-33, 2-34](#)

## flooding controls

- configuring [4-18](#)

- illustrated [4-19](#)

flow control, configuring [3-49](#)

## forwarding

- controlling (SNMP) [2-37](#)

- delay [4-89, 4-93](#)

- port groups [4-12](#)

- restrictions [4-14](#)

- source-based, illustrated [4-12](#)

- see also broadcast storm control

forwarding window, static address [4-55](#)

FTP, accessing MIB files with [2-35](#)

---

## G

get-next-request operation [2-36, 2-37](#)

get-request operation [2-36, 2-37](#)

get-response operation [2-37](#)

## Gigabit Ethernet

- ports, configuring flow control on [3-50](#)

- settings [3-42](#)

- trunks [5-29](#)

global configuration mode [2-26](#)

graphing bytes [6-2](#)

## graphs

- bandwidth [2-19](#)

- link utilization [6-1](#)

- percent utilization [6-2](#)

- poll result [2-36](#)

---

## H

### hardware

- supported switches [1-3](#)

hello BPDU interval [4-92](#)

### hello time

- changing [4-92](#)

- defined [4-89](#)

help, getting [2-20, 2-30](#)

Help button [2-4](#)

history group, in RMON [2-38](#)

home page, VSM [4-10](#)

hops, configuring [4-64](#)

### host names

- abbreviations appended to [3-21](#)

- changes to [3-10](#)

- changing [3-37](#)

- to address mappings [4-39](#)

Hot Standby Router Protocol

- see HSRP

HSRP [3-17, 3-22](#)

see also standby group

---

## icons

Cluster Builder [2-7](#)

Cluster Manager toolbar [2-19](#)

Cluster View [2-7](#)

## IEEE 802.1Q

configuration considerations [5-30](#)

interaction with other features [5-30](#)

native VLAN for untagged traffic [5-36](#)

overview [5-29](#)

## IEEE 802.1Q trunks [5-30](#)

## IGMP snooping [4-64](#)

configuring a multicast router port [4-69](#)

disabling [4-66](#)

enabling [4-66](#)

joining a multicast group [4-70](#)

leaving a multicast group [4-76](#)

## Immediate Leave [4-68](#)

defined [4-68](#)

disable [4-69](#)

enable [4-69](#)

## ingress port scheduling [5-37](#)

## interface configuration mode [2-27](#)

## interfaces

Cluster Builder [2-5](#)

Cluster View [2-5](#)

IOS supported [1-4](#)

## Internet Group Management Protocol

see IGMP snooping

inventory, displaying [3-33](#)

## IOS

see software and upgrading [3-2](#)

## IP addresses

and admittance to standby groups [3-20](#)

candidate [3-4](#)

discovering [4-47](#)

management VLAN [3-4](#)

point of access [3-1](#)

in redundant clusters [3-18](#)

removing [4-29](#)

see also IP information

## IP information

assigning [4-28](#)

configuring [4-26](#)

displaying [3-33](#)

removing [4-29](#)

## IP Management window [4-27](#)

## IP setup program [7-10, 7-12](#)

## IPX server time-out, and Port Fast [4-95](#)

---

## L

LEDs, monitoring [3-39, 3-41](#)

line configuration mode [2-27](#)



## link

- graph, illustrated [6-3](#)

- utilization graphs [6-1](#)

- link icons, Cluster Builder and Cluster View [2-7](#)

- link information, displaying [3-34](#)

## load sharing

- STP, described [5-43](#)

- using STP path cost [5-46](#)

- using STP port priorities [5-44](#)

- location of displayed switches [3-32](#)

- location of switches, displaying [3-33](#)

- login authentication, configuring [4-104](#)

---

**M**

## MAC addresses

- adding secure [4-52](#)

- aging time [4-50](#)

- discovering [4-47, 4-50](#)

- MAC address tables, managing [4-49](#)

- management interface features [2-1](#)

- management options [1-4](#)

## management VLAN

- changes, understanding [3-4](#)

- changing [3-4, 3-34](#)

- configuring [3-37](#)

- described [5-4](#)

- IP address [3-4](#)

- Management VLAN window [3-36](#)

## map

- see also network map

- membership mode, VLAN port [5-3](#)

## member switches

- accessing [5-6, 5-28](#)

- adding

- with Cluster Builder [3-12](#)

- from the command line [3-14](#)

- to standby group [3-24](#)

- assigning host names to [3-10](#)

- defined [1-3](#)

- displaying inventory of [3-33](#)

- managing [2-29](#)

- order [3-31](#)

- passwords, inherited [3-11](#)

- recovering from lost connectivity [7-14](#)

- removing

- from standby group [3-25](#)

- upgrading [3-57, 3-58](#)

- see also candidates, command switch

## menu options

- Cluster Builder [2-7](#)

- Cluster Manager [2-15](#)

- Cluster View [2-7, 2-14](#)

- VSM [2-22](#)

- see also pop-up menus

- messages, CLI error [2-31](#)

message severity levels  
    description [A-2](#)  
    table [A-2](#)

MIB files, accessing [2-35](#)

MIB objects, accessing [2-34](#)

MIB variables, accessing [2-35](#)

mismatches, autonegotiation [7-1](#)

mnemonic code [A-2](#)

Mode button [2-21, 3-39, 3-40](#)

model numbers, displaying [3-33](#)

modes  
    command [2-25](#)  
    VLAN port membership [5-3](#)  
    VTP  
        see VTP modes

Modify button [2-4](#)

modules  
    installed, displaying [3-33](#)

monitoring  
    devices with Cluster Manager [2-14](#)  
    LEDs [3-39, 3-41](#)  
    ports [3-38, 4-15](#)  
    traffic [4-15](#)  
    VTP [5-18](#)

multicast groups  
    joining [4-70](#)  
    leaving [4-76](#)

multicast traffic, and protected ports [4-101](#)

---

## N

name command [3-22](#)

NAT [3-9](#)

native VLANs [5-36](#)

NCPs [4-105](#)

Network Address Translation  
    see NAT

Network Control Protocols (NCPs) [4-105](#)

network map  
    creating [3-30](#)  
    saving [3-30](#)

Network Time Protocol. See NTP

no commands, using [2-31](#)

Note described [xvii](#)

NTP  
    authentication, enabling [4-26](#)  
    broadcast-client mode [4-26](#)  
    client [4-25](#)  
    configuring [4-24](#)  
    described [4-24](#)  
    illustrated [4-25](#)

---

## O

OK button [2-4](#)

online help, displaying [2-4](#)

order, switch [3-31](#)

---

## P

### packets

- graphing [6-2](#)

- parallel links [5-43](#)

### passwords

- candidate switch [3-6](#)

- changing [4-11](#)

- community strings [4-42](#)

- member switch, inherited [3-11](#)

- recovery of [3-19, 7-6](#)

- setting [2-27](#)

- TACACS+ server [4-102](#)

- VTP domain [5-11](#)

- path cost [4-96, 4-97, 5-46](#)

- polling interval [3-31](#)

- poll results, graphing [2-36](#)

### pop-up menus

- Cluster Builder candidate [2-11](#)

- Cluster Builder link [2-12](#)

- Cluster Builder member [2-12](#)

- Cluster Manager device [2-18](#)

- Cluster Manager port [2-17](#)

- port-connection information, displaying [3-34](#)

### Port Fast

- configuring [3-38](#)

- enabling [4-95, 4-97](#)

### port groups

- and trunks [5-31](#)

- configuring [3-38](#)

- configuring static addresses  
(EtherChannel) [4-57](#)

- creating EtherChannel [4-11, 4-15](#)

- destination-based [4-12, 4-57](#)

- forwarding [4-12](#)

- restrictions on forwarding [4-14](#)

- source-based [4-12, 4-57](#)

- see also ports

- port membership modes, VLAN [5-3](#)

- port-monitoring conflicts with trunks [5-30](#)

- port pop-up menu [2-17](#)

### ports

- configuration guidelines [3-41](#)

#### configuring

- through Cluster Manager [3-38, 3-42](#)

- multiple mixed [3-43](#)

- with port pop-up menu [2-17](#)

- protected ports [4-100](#)

- trunk [5-31](#)

- voice [4-108](#)

- through VSM [2-21](#)

#### Gigabit Ethernet

- configuring flow control on [3-50](#)

- monitoring [3-38, 5-30](#)

- priority [4-98, 5-37, 5-44](#)

- protected ports [4-100](#)

- secure [4-60, 5-31](#)

security

- described [4-58](#)
- disabling [4-62](#)
- enabling [4-61](#)

speed, setting and checking [3-38, 3-41](#)

static-access [5-3, 5-5, 5-28](#)

STP parameters, changing [4-93](#)

trunk

- configuring [5-31](#)
- disabling [5-34](#)

trunks [5-3, 5-29](#)

VLAN, displaying [3-50](#)

VLAN assignments [5-5, 5-28](#)

see also port groups

port scheduling [5-37](#)

preempt command [3-22](#)

priority

- assigning standby [3-22](#)
- modifying switch [4-91](#)

port

- described [5-37](#)
- modifying [4-96, 4-98](#)

standby group member [3-20](#)

privileged EXEC mode [2-26](#)

privilege levels

- command switch [2-29](#)
- inherited [3-11](#)
- mapping on member switches [2-29, 3-11](#)
- setting [2-27](#)

specifying [2-28](#)

web-based management application [2-2](#)

properties, displaying switch [3-33](#)

protected ports, configuring [4-100](#)

publications, related [xvii](#)

---

## Q

QoS

- egress port scheduling [5-38](#)
- ingress port scheduling [5-37, 5-42](#)

---

## R

rcommand [2-29](#)

recovery procedures [7-4](#)

redundancy

- cluster [3-2, 3-17](#)
- STP [4-83](#)
  - path cost [5-46](#)
  - port priority [5-44](#)
  - UplinkFast [4-84](#)

redundancy-enable command [3-22](#)

remote devices without autonegotiation,  
connecting to [3-42](#)

remove vlan-list parameter [5-34](#)

removing

- dynamic address entries [4-52](#)
- IP information [4-29](#)

- secure addresses [4-55](#)
- standby group from network [3-26](#)
- static addresses [4-55, 4-58](#)
- switches from a standby group [3-25](#)
- Requested and Actual settings [3-41](#)
- RMON
  - configuring [4-108](#)
  - supported groups [2-38](#)
- root guard [4-98, 4-99](#)

---

## S

- saving
  - cluster configuration [3-33](#)
  - network map [3-30](#)
- secure address count [4-60](#)
- secure addresses
  - adding [4-52, 4-54](#)
  - described [4-52](#)
  - removing [4-55](#)
- secure ports
  - address-security violations [4-59](#)
  - disabling [4-62](#)
  - enabling [4-58, 4-61](#)
  - maximum secure address count [4-60](#)
  - and trunks [5-31](#)
- security
  - port [4-58](#)
  - TACACS+ [4-102](#)
  - violations, address [4-59](#)
- Serial Line Internet Protocol (SLIP) [4-105](#)
- serial numbers, displaying [3-33](#)
- server, domain name [4-41](#)
- server mode, VTP [5-8](#)
- server time-out, and Port Fast [4-95](#)
- set-request operation [2-36, 2-37](#)
- setting
  - see configuring
- settings
  - cluster, initial [3-30](#)
  - default, changing [4-3](#)
  - duplex [3-38, 3-41, 3-49](#)
  - multiple mixed port [3-43](#)
  - port, monitoring [3-39](#)
  - Requested and Actual [3-41](#)
  - speed [3-49](#)
  - user, changing [3-31](#)
- setup program [7-10, 7-12](#)
- severity levels
  - description [A-2](#)
  - table [A-2](#)
- show cluster candidates command [3-14](#)
- show cluster members command [2-29, 3-14](#)
- SLIP [4-105](#)
- small to medium-sized business workgroup
  - aggregation [1-7](#)
- SNMP [3-59](#)
  - accessing MIB variables with [2-35](#)
  - agent [3-60](#)

- community strings
    - changes to [3-10](#)
    - configuring [3-60, 4-42](#)
  - configuring for
    - cluster members [3-59](#)
    - single switches [4-41](#)
  - disabling [3-60](#)
  - enabling [3-60](#)
  - enabling and disabling [4-42](#)
  - management, using [2-34](#)
  - managing clusters with [2-37](#)
  - network management platforms [1-5](#)
  - RMON groups [2-38](#)
  - trap managers, configuring [3-63, 4-44](#)
  - trap types [3-63, 3-64, 4-45](#)
- SNMP Configuration window, displaying [2-20](#)
- SNMP Manager, illustrated [3-61, 3-62](#)
- software
- recovery procedures [7-5](#)
  - reloading [3-59](#)
  - requirements for
    - changing management VLAN [3-36](#)
    - joining standby groups [3-20](#)
  - to support clustering [3-2](#)
  - upgrading switch [3-51](#)
  - version numbers, displaying [3-33](#)
  - see also upgrading
- Software Upgrade window [2-20](#)
- source-based forwarding [4-14](#)
- source-based port groups [4-12, 4-57](#)
- SPAN
- described [4-15](#)
  - disabling [4-18](#)
  - enabling [4-17](#)
  - ports, restrictions [4-2](#)
- Spanning-Tree Protocol
- see STP
- spanning-tree rootguard command [4-99](#)
- speed, setting [3-38, 3-41, 3-49](#)
- splash screen, displaying at startup [3-31](#)
- standalone switches
- configuring [4-9](#)
- Standby Command Configuration window [3-20, 3-21](#)
- standby command switch requirements [3-20](#)
- standby group
- adding switches to [3-24](#)
  - configuration guidelines [3-22](#)
  - configuring [3-17, 3-19, 3-22](#)
  - priority, configuring [3-20](#)
  - removing from network [3-26](#)
  - removing switches from [3-25](#)
- startup configuration, copying to PC or server [3-52](#)
- static-access ports
- assigning to VLAN [5-5, 5-28](#)
  - described [5-5](#)
  - VLAN membership combinations [5-3](#)
- static addresses

- adding [4-55, 4-57](#)
  - configuring for EtherChannel port groups [4-57](#)
  - described [4-49, 4-55](#)
  - removing [4-58](#)
  - see also static address
  - static address forwarding restrictions [4-14](#)
  - static address forwarding window [4-55](#)
  - statistics, VTP [5-18](#)
  - statistics group, in RMON [2-38](#)
  - status, monitoring port [3-38](#)
  - STP
    - BPDU message interval [4-92](#)
    - configuring [4-80](#)
    - disabling [4-83, 4-84](#)
    - forwarding delay timer [4-93](#)
    - hello BPDU interval [4-92](#)
    - implementation type [4-90](#)
    - load sharing
      - overview [5-43](#)
      - using path costs [5-46](#)
      - using port priorities [5-44](#)
    - number of supported instances [5-2](#)
    - parameters [4-80](#)
    - path cost
      - changing [4-97](#)
      - configuring [5-48](#)
    - Port Fast
      - enabling [4-95, 4-97](#)
    - port grouping parameters [4-13, 5-31](#)
    - port parameters, changing [4-93](#)
    - port priority [4-98, 5-45](#)
    - redundant connectivity [4-83](#)
    - redundant links with UplinkFast [4-84](#)
    - root guard [4-98, 4-99](#)
    - supported number of spanning-tree instances [4-80](#)
    - switch priority [4-91](#)
    - UplinkFast [4-84, 4-87](#)
    - VLAN parameters described [4-87](#)
    - stp-list parameter [4-80](#)
  - Sun Microsystems
    - URL for required plug-in [4-9](#)
  - switches
    - see candidates, command switch, member switches
  - Switch Port Analyzer (SPAN)
    - disabling [4-18](#)
    - enabling [4-15, 4-17](#)
    - illustrated [4-16](#)
  - switchport command [5-33](#)
  - system date and time [4-22](#)
- 
- ## T
- tables
    - message severity levels [A-2](#)
    - variable fields [A-3](#)
  - TACACS+
    - AAA accounting commands [4-106](#)

- AAA authorization commands [4-105](#)
  - configuring [4-101](#)
  - initializing [4-104](#)
  - server, creating [4-103](#)
- tacacs-server host command [4-103](#)
- tacacs-server retransmit command [4-103, 4-107](#)
- tacacs-server timeout command [4-103](#)
- Telnet, starting from browser [2-33](#)
- TFTP server, upgrading multiple switches with [3-52](#)
- time
  - daylight saving [4-23](#)
  - setting [4-22](#)
- time zones [4-22](#)
- TLV [5-10](#)
- Token Ring VLANs
  - overview [5-20](#)
  - TrBRF [5-10, 5-22](#)
  - TrCRF [5-10, 5-23](#)
- toolbar icons
  - Cluster Builder [2-6](#)
  - Cluster Manager [2-19](#)
  - Cluster View [2-6](#)
- topology [3-30](#)
  - see also network map
- traceback reports [A-4](#)
- traffic
  - forwarding, and protected ports [4-100](#)
  - monitoring [4-15](#)
  - reducing flooded [4-18](#)
  - transmit queue [5-38](#)
- transparent mode, VTP [5-8, 5-16](#)
- trap managers
  - adding [4-44, 4-47](#)
  - configuring [3-63, 4-44](#)
  - supported [3-63](#)
- traps [2-37, 3-63, 4-45](#)
- TrBRF VLAN defaults and ranges [5-22](#)
- TrCRF VLAN defaults and ranges [5-23](#)
- troubleshooting
  - IOS [7-1](#)
  - with CiscoWorks2000 [2-36](#)
- trunk ports
  - configuring [5-31](#)
  - disabling [5-34](#)
- trunks
  - allowed-VLAN list [5-34](#)
  - configuration conflicts [5-30](#)
  - configuring [5-33](#)
  - disabling [5-34](#)
  - IEEE 802.1Q [5-30](#)
  - interacting with other features [5-30](#)
  - load sharing using
    - STP path costs [5-46](#)
    - STP port priorities [5-44](#)
  - native VLAN for untagged traffic [5-36](#)
  - overview [5-29](#)
  - parallel [5-46](#)
  - VLAN, overview [5-29](#)



VLAN membership combinations [5-4](#)  
 TTY traps [3-63, 4-45](#)

## U

UDLD [4-100](#)  
 unicast traffic, and protected ports [4-101](#)  
 UniDirectional Link Detection  
   see UDLD  
 Unrecognized Type-Length-Value (TLV)  
   support [5-10](#)  
 upgrading  
   1900 and 2820 member switches [3-58](#)  
   2900, 2950, and 3500 member switches [3-57](#)  
   conflicts while [3-55](#)  
   multiple switches with TFTP [3-52](#)  
   software  
     with CLI [3-55](#)  
     with VSM [3-59](#)  
   standalone switches [3-55](#)  
   switch software [3-51](#)  
 UplinkFast  
   enabling [4-87](#)  
   redundant links [4-84](#)  
 user EXEC mode [2-26](#)  
 user settings [3-31](#)  
 User Settings window, displaying [2-20](#)  
 utilization graphs [6-1](#)

## V

variable fields  
   definition [A-3](#)  
   table [A-3](#)  
 version-dependent transparent mode [5-10](#)  
 virtual IP address  
   HSRP [3-18](#)  
   standby group member [3-21](#)  
   see also IP addresses  
 VLAN  
   port membership modes [5-3](#)  
   trunks, overview [5-29](#)  
 VLAN database mode [2-26](#)  
 VLAN ID, discovering [4-47, 4-50](#)  
 VLAN membership  
   combinations [5-3](#)  
   described [5-4](#)  
   displaying [3-50](#)  
   modes [5-3](#)  
   port group parameters [4-13](#)  
   traps [3-63, 4-45](#)  
   see also dynamic ports VLAN membership  
 VLAN membership combinations [5-3](#)  
 VLAN Membership window [2-20](#)  
 VLANs  
   802.1Q considerations [5-30](#)  
   adding to database [5-25](#)  
   aging dynamic addresses [4-83](#)

- allowed on trunk [5-34](#)
- changing [5-26](#)
- configuration guidelines [5-20](#)
- configuring [5-1, 5-5, 5-24](#)
- default configuration [5-21](#)
- deleting from database [5-27](#)
- described [5-1](#)
- displaying [3-50](#)
- illustrated [5-2](#)
- MAC addresses [4-50](#)
- modifying [5-26](#)
- native, configuring [5-36](#)
- number supported [5-2](#)
- static-access ports [5-5, 5-26, 5-28](#)
- STP parameters, changing [4-87](#)
- supported [5-2](#)
- Token Ring [5-20](#)
- trunks configured with other features [5-30](#)
  - see also trunks
- VTP database and [5-19](#)
- VTP modes [5-8](#)
- See also management VLAN
- voice ports, configuring [4-108](#)
- VSM
  - accessing [4-9](#)
  - conflicts while upgrading [3-55](#)
  - home page [2-21, 4-10](#)
  - menu options [2-22](#)
  - overview [1-4](#)
  - privilege level [2-28](#)
  - using [2-20](#)
- VTP
  - advertisements [5-9](#)
  - configuration guidelines [5-10](#)
  - configuring [5-12](#)
  - consistency checks [5-10](#)
  - database [5-19, 5-24](#)
  - default configuration [5-12](#)
  - described [5-6](#)
  - disabling [5-16](#)
  - domain names [5-10](#)
  - domains [5-7](#)
  - modes
    - client [5-8](#)
    - configuring [5-15](#)
    - server [5-8, 5-14](#)
    - transitions [5-8](#)
    - transparent [5-6, 5-8, 5-16](#)
  - monitoring [5-18](#)
  - statistics [5-18](#)
  - Token Ring support [5-10](#)
  - transparent mode, configuring [5-16](#)
  - traps [3-63, 4-45](#)
  - using [5-6](#)
  - version, determining [5-11](#)
  - version 1 [5-10](#)

## version 2

- configuration guidelines [5-11](#)

- disabling [5-18](#)

- enabling [5-17](#)

- overview [5-10](#)

- VLAN parameters [5-19](#)

---

## W

- web-based management, using [2-2](#)

### Weighted Round Robin

- see WRR

### WRR

- configuring [5-43](#)

- defining [5-39](#)

- description [5-39](#)

---

## X

- Xmodem protocol [7-5](#)

