Catalyst 3750 Metro Switch Software Configuration Guide

Cisco IOS Release 12.2(55)SE
August 2010
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.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at
www.cisco.com/go/trademarks. Third party trademarks mentioned 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. (1005R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the
document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Catalyst 3750 Metro Switch Software Configuration Guide
©2006—2010 Cisco Systems, Inc. All rights reserved.
## CONTENTS

**Preface**  xlvii

**Audience**  xlvii

**Purpose**  xlvii

**Conventions**  xlvii

**Related Publications**  xlviii

**Obtaining Documentation and Submitting a Service Request**  xlix

### CHAPTER 1

**Overview**  1-1

**Features**  1-1

- Performance Features  1-2
- Management Options  1-3
- Manageability Features  1-3
- Availability Features  1-4
- VLAN Features  1-6
- Layer 2 Virtual Private Network (VPN) Services  1-6
- Layer 3 VPN Services  1-7
- Security Features  1-7
- QoS Features  1-8
- Layer 3 Features  1-10
- Monitoring Features  1-11

**Default Settings After Initial Switch Configuration**  1-12

**Network Configuration Examples**  1-14

- Multidwelling or Ethernet-to-the Subscriber Network  1-15
- Layer 2 VPN Application  1-16
- Layer 3 VPN Application  1-17

**Where to Go Next**  1-18

### CHAPTER 2

**Using the Command-Line Interface**  2-1

- Understanding Command Modes  2-1
- Understanding the Help System  2-3
- Understanding Abbreviated Commands  2-3
- Understanding no and default Forms of Commands  2-4
- Understanding CLI Error Messages  2-4
Contents

CHAPTER 2
Using Command History 2-4
  Changing the Command History Buffer Size 2-5
  Recalling Commands 2-5
  Disabling the Command History Feature 2-5

Using Editing Features 2-6
  Enabling and Disabling Editing Features 2-6
  Editing Commands through Keystrokes 2-6
  Editing Command Lines that Wrap 2-8

Searching and Filtering Output of show and more Commands 2-8
Accessing the CLI 2-9

CHAPTER 3
Assigning the Switch IP Address and Default Gateway 3-1
  Understanding the Boot Process 3-1
  Assigning Switch Information 3-2
    Default Switch Information 3-3
    Understanding DHCP-Based Autoconfiguration 3-3
      DHCP Client Request Process 3-4
    Understanding DHCP-based Autoconfiguration and Image Update 3-5
      DHCP Autoconfiguration 3-5
      DHCP Auto-Image Update 3-5
      Limitations and Restrictions 3-5
  Configuring DHCP-Based Autoconfiguration 3-6
    DHCP Server Configuration Guidelines 3-6
    Configuring the TFTP Server 3-7
    Configuring the DNS 3-7
    Configuring the Relay Device 3-8
    Obtaining Configuration Files 3-8
    Example Configuration 3-9
  Configuring the DHCP Auto Configuration and Image Update Features 3-11
    Configuring DHCP Autoconfiguration (Only Configuration File) 3-11
    Configuring DHCP Auto-Image Update (Configuration File and Image) 3-12
  Configuring the Client 3-13
  Manually Assigning IP Information 3-14

Checking and Saving the Running Configuration 3-15
Modifying the Startup Configuration 3-15
  Default Boot Configuration 3-15
  Automatically Downloading a Configuration File 3-16
  Specifying the Filename to Read and Write the System Configuration 3-16
  Booting Manually 3-17
Booting a Specific Software Image 3-17
Controlling Environment Variables 3-18
Scheduling a Reload of the Software Image 3-19
Configuring a Scheduled Reload 3-19
Displaying Scheduled Reload Information 3-20

CHAPTER 4
Configuring Cisco IOS Configuration Engine 4-1
Understanding Cisco Configuration Engine Software 4-1
Configuration Service 4-2
Event Service 4-3
NameSpace Mapper 4-3
What You Should Know About the CNS IDs and Device Hostnames 4-3
ConfigID 4-3
DeviceID 4-4
Hostname and DeviceID 4-4
Using Hostname, DeviceID, and ConfigID 4-4
Understanding Cisco IOS Agents 4-5
Initial Configuration 4-5
Incremental (Partial) Configuration 4-6
Synchronized Configuration 4-6
Configuring Cisco IOS Agents 4-6
Enabling Automated CNS Configuration 4-6
Enabling the CNS Event Agent 4-7
Enabling the Cisco IOS CNS Agent 4-9
Enabling an Initial Configuration 4-9
Enabling a Partial Configuration 4-13
Upgrading Devices with Cisco IOS Image Agent 4-14
Prerequisites for the CNS Image Agent 4-14
Restrictions for the CNS Image Agent 4-14
Displaying CNS Configuration 4-15

CHAPTER 5
Administering the Switch 5-1
Managing the System Time and Date 5-1
Understanding the System Clock 5-1
Understanding Network Time Protocol 5-2
Configuring NTP 5-3
Default NTP Configuration 5-4
Configuring NTP Authentication 5-4
Configuring NTP Associations 5-5
Contents

CHAPTER 5

Configuring NTP Broadcast Service 5-6
Configuring NTP Access Restrictions 5-8
Configuring the Source IP Address for NTP Packets 5-10
Displaying the NTP Configuration 5-10
Configuring Time and Date Manually 5-11
  Setting the System Clock 5-11
  Displaying the Time and Date Configuration 5-11
  Configuring the Time Zone 5-12
  Configuring Summer Time (Daylight Saving Time) 5-13
Configuring a System Name and Prompt 5-14
  Default System Name and Prompt Configuration 5-15
Configuring a System Name 5-15
Understanding DNS 5-15
  Default DNS Configuration 5-16
  Setting Up DNS 5-16
  Displaying the DNS Configuration 5-17
Creating a Banner 5-17
  Default Banner Configuration 5-17
  Configuring a Message-of-the-Day Login Banner 5-18
  Configuring a Login Banner 5-19
Managing the MAC Address Table 5-19
  Building the Address Table 5-20
  MAC Addresses and VLANs 5-20
  Default MAC Address Table Configuration 5-21
  Changing the Address Aging Time 5-21
  Removing Dynamic Address Entries 5-22
  Configuring MAC Address Change Notification Traps 5-22
  Configuring MAC Address Move Notification Traps 5-24
  Configuring MAC Threshold Notification Traps 5-26
  Adding and Removing Static Address Entries 5-27
  Configuring Unicast MAC Address Filtering 5-28
  Disabling MAC Address Learning on a VLAN 5-29
  Displaying Address Table Entries 5-30
Managing the ARP Table 5-31

CHAPTER 6

Configuring SDM Templates 6-1
  Understanding the SDM Templates 6-1
  Dual IPv4 and IPv6 SDM Templates 6-2
  Configuring the Switch SDM Template 6-3
  Default SDM Template 6-3
CHAPTER 7

Configuring Switch-Based Authentication

Preventing Unauthorized Access to Your Switch

Protecting Access to Privileged EXEC Commands

Default Password and Privilege Level Configuration

Setting or Changing a Static Enable Password

Protecting Enable and Enable Secret Passwords with Encryption

Disabling Password Recovery

Setting a Telnet Password for a Terminal Line

Configuring Username and Password Pairs

Configuring Multiple Privilege Levels

Setting the Privilege Level for a Command

Changing the Default Privilege Level for Lines

Logging into and Exiting a Privilege Level

Controlling Switch Access with TACACS+

Understanding TACACS+

TACACS+ Operation

Configuring TACACS+

Default TACACS+ Configuration

Identifying the TACACS+ Server Host and Setting the Authentication Key

Configuring TACACS+ Login Authentication

Configuring TACACS+ Authorization for Privileged EXEC Access and Network Services

Starting TACACS+ Accounting

Displaying the TACACS+ Configuration

Controlling Switch Access with RADIUS

Understanding RADIUS

RADIUS Operation

Configuring RADIUS

Default RADIUS Configuration

Identifying the RADIUS Server Host

Configuring RADIUS Login Authentication

Defining AAA Server Groups

Configuring RADIUS Authorization for User Privileged Access and Network Services

Starting RADIUS Accounting

Configuring Settings for All RADIUS Servers

Configuring the Switch to Use Vendor-Specific RADIUS Attributes
Contents

Configuring the Switch for Vendor-Proprietary RADIUS Server Communication 7-29
Configuring RADIUS Server Load Balancing 7-30
Displaying the RADIUS Configuration 7-30
Controlling Switch Access with Kerberos 7-31
Understanding Kerberos 7-31
Kerberos Operation 7-33
  Authenticating to a Boundary Switch 7-33
  Obtaining a TGT from a KDC 7-34
  Authenticating to Network Services 7-34
Configuring Kerberos 7-34
Configuring the Switch for Local Authentication and Authorization 7-35
Configuring the Switch for Secure Shell 7-36
Understanding SSH 7-36
  SSH Servers, Integrated Clients, and Supported Versions 7-36
  Limitations 7-37
Configuring SSH 7-37
  Configuration Guidelines 7-37
  Setting Up the Switch to Run SSH 7-38
  Configuring the SSH Server 7-39
Displaying the SSH Configuration and Status 7-40
Configuring the Switch for Secure Socket Layer HTTP 7-40
Understanding Secure HTTP Servers and Clients 7-40
  Certificate Authority Trustpoints 7-41
  CipherSuites 7-42
Configuring Secure HTTP Servers and Clients 7-42
  Default SSL Configuration 7-43
  SSL Configuration Guidelines 7-43
  Configuring a CA Trustpoint 7-43
  Configuring the Secure HTTP Server 7-44
  Configuring the Secure HTTP Client 7-46
  Displaying Secure HTTP Server and Client Status 7-46
Configuring the Switch for Secure Copy Protocol 7-46
  Information About Secure Copy 7-47

CHAPTER 8
Configuring IEEE 802.1x Port-Based Authentication 8-1
Understanding IEEE 802.1x Port-Based Authentication 8-1
  Device Roles 8-2
  Authentication Initiation and Message Exchange 8-3
  Ports in Authorized and Unauthorized States 8-4
802.1x Accounting 8-5
Supported Topologies 8-5
802.1x Readiness Check 8-6
802.1x with Port Security 8-6
802.1x with Voice VLAN Ports 8-7
802.1x with VLAN Assignment 8-8
802.1x with Guest VLAN 8-9
802.1x with Restricted VLAN 8-10
802.1x with Per-User ACLs 8-11
802.1x User Distribution 8-12
   802.1x User Distribution Configuration Guidelines 8-12
   802.1x Supplicant and Authenticator Switches with Network Edge Access Topology (NEAT) 8-12
Common Session ID 8-13
Configuring IEEE 802.1x Authentication 8-14
   Default 802.1x Configuration 8-15
   802.1x Configuration Guidelines 8-16
      Maximum Number of Allowed Devices Per Port 8-17
Configuring 802.1x Readiness Check 8-17
Configuring IEEE 802.1x Violation Modes 8-18
Configuring IEEE 802.1x Authentication 8-19
Configuring the Switch-to-RADIUS-Server Communication 8-20
Configuring Periodic Re-Authentication 8-22
Manually Re-Authenticating a Client Connected to a Port 8-22
Changing the Quiet Period 8-22
Changing the Switch-to-Client Retransmission Time 8-23
Setting the Switch-to-Client Frame-Retransmission Number 8-24
Setting the Re-Authentication Number 8-25
Configuring the Host Mode 8-25
Configuring a Guest VLAN 8-26
Configuring a Restricted VLAN 8-27
Resetting the 802.1x Configuration to the Default Values 8-29
Configuring 802.1x Accounting 8-29
Configuring 802.1x User Distribution 8-30
Configuring an Authenticator and a Supplicant Switch with NEAT 8-31
   Configuring NEAT with ASP 8-32
   Configuring 802.1x Authentication with Downloadable ACLs and Redirect URLs 8-33
      Configuring Downloadable ACLs 8-33
      Configuring a Downloadable Policy 8-34
Displaying 802.1x Statistics and Status 8-35
CHAPTER 9

Configuring Interface Characteristics 9-1
Understanding Interface Types 9-1
Port-Based VLANs 9-2
Switch Ports 9-2
Access Ports 9-2
Trunk Ports 9-3
Tunnel Ports 9-4
Routed Ports 9-4
Switch Virtual Interfaces 9-4
EtherChannel Port Groups 9-5
Connecting Interfaces 9-5
Using Interface Configuration Mode 9-7
Procedures for Configuring Interfaces 9-7
Configuring a Range of Interfaces 9-8
Configuring and Using Interface Range Macros 9-10
Configuring Ethernet Interfaces 9-11
Default Ethernet Interface Configuration 9-11
Configuring Interface Speed and Duplex Mode 9-12
Speed and Duplex Configuration Guidelines 9-13
Setting the Interface Speed and Duplex Parameters 9-13
Configuring IEEE 802.3x Flow Control 9-14
Configuring Auto-MDIX on a Port 9-15
Adding a Description for an Interface 9-17
Configuring Layer 3 Interfaces 9-17
Configuring the System MTU 9-19
Monitoring and Maintaining the Interfaces 9-22
Monitoring Interface Status 9-22
Clearing and Resetting Interfaces and Counters 9-23
Shutting Down and Restarting the Interface 9-23

CHAPTER 10

Configuring Smartports Macros 10-1
Understanding Smartports Macros 10-1
Configuring Smartports Macros 10-2
Default Smartports Macro Configuration 10-2
Smartports Macro Configuration Guidelines 10-2
Creating Smartports Macros 10-4
Applying Smartports Macros 10-5
Applying Cisco-Default Smartports Macros 10-6
Displaying Smartports Macros 10-8

CHAPTER 11

Configuring VLANs 11-1

Understanding VLANs 11-1
  Supported VLANs 11-2
  VLAN Port Membership Modes 11-3
Configuring Normal-Range VLANs 11-4
  Token Ring VLANs 11-6
  Normal-Range VLAN Configuration Guidelines 11-6
  Saving VLAN Configuration 11-7
  Default Ethernet VLAN Configuration 11-7
  Creating or Modifying an Ethernet VLAN 11-8
  Deleting a VLAN 11-9
  Assigning Static-Access Ports to a VLAN 11-10
Configuring Extended-Range VLANs 11-11
  Default VLAN Configuration 11-11
  Extended-Range VLAN Configuration Guidelines 11-11
  Creating an Extended-Range VLAN 11-12
  Creating an Extended-Range VLAN with an Internal VLAN ID 11-13
Displaying VLANs 11-14
Configuring VLAN Trunks 11-15
  Trunking Overview 11-15
    Encapsulation Types 11-16
    IEEE 802.1Q Configuration Considerations 11-18
  Default Layer 2 Ethernet Interface VLAN Configuration 11-18
  Configuring an Ethernet Interface as a Trunk Port 11-19
    Interaction with Other Features 11-19
    Configuring a Trunk Port 11-20
    Defining the Allowed VLANs on a Trunk 11-21
    Changing the Pruning-Eligible List 11-22
    Configuring the Native VLAN for Untagged Traffic 11-23
    Configuring Trunk Ports for Load Sharing 11-23
    Load Sharing Using STP Port Priorities 11-24
    Load Sharing Using STP Path Cost 11-26
Configuring VMPS 11-27
  Understanding VMPS 11-28
    Dynamic-Access Port VLAN Membership 11-28
  Default VMPS Client Configuration 11-29
  VMPS Configuration Guidelines 11-29
CHAPTER 11
Configuring the VMPS Client 11-30
  Entering the IP Address of the VMPS 11-30
  Configuring Dynamic-Access Ports on VMPS Clients 11-30
  Reconfirming VLAN Memberships 11-31
  Changing the Reconfirmation Interval 11-31
  Changing the Retry Count 11-32
  Monitoring the VMPS 11-32
  Troubleshooting Dynamic-Access Port VLAN Membership 11-33
  VMPS Configuration Example 11-33

CHAPTER 12
Configuring VTP 12-1
  Understanding VTP 12-1
    The VTP Domain 12-2
    VTP Modes 12-3
    VTP Advertisements 12-3
    VTP Version 2 12-4
    VTP Pruning 12-4
  Configuring VTP 12-6
    Default VTP Configuration 12-6
    VTP Configuration Guidelines 12-6
      Domain Names 12-7
      Passwords 12-7
      VTP Version 12-8
      Configuration Requirements 12-8
    Configuring a VTP Server 12-8
    Configuring a VTP Client 12-9
    Disabling VTP (VTP Transparent Mode) 12-10
    Enabling VTP Version 2 12-11
    Enabling VTP Pruning 12-12
    Adding a VTP Client Switch to a VTP Domain 12-12
    Monitoring VTP 12-13

CHAPTER 13
Configuring Private VLANs 13-1
  Understanding Private VLANs 13-1
    IP Addressing Scheme with Private VLANs 13-3
    Private VLANs across Multiple Switches 13-4
    Private-VLAN Interaction with Other Features 13-5
      Private VLANs and Unicast, Broadcast, and Multicast Traffic 13-5
      Private VLANs and SVIs 13-5
Configuring Private VLANs  13-6
- Tasks for Configuring Private VLANs  13-6
- Default Private-VLAN Configuration  13-6
- Private-VLAN Configuration Guidelines  13-7
  - Secondary and Primary VLAN Configuration  13-7
  - Private-VLAN Port Configuration  13-8
  - Limitations with Other Features  13-9
- Configuring and Associating VLANs in a Private VLAN  13-10
- Configuring a Layer 2 Interface as a Private-VLAN Host Port  13-11
- Configuring a Layer 2 Interface as a Private-VLAN Promiscuous Port  13-12
- Mapping Secondary VLANs to a Primary VLAN Layer 3 VLAN Interface  13-13

Monitoring Private VLANs  13-14

CHAPTER 14
Configuring Voice VLAN  14-1
- Understanding Voice VLAN  14-1
  - Cisco IP Phone Voice Traffic  14-2
  - Cisco IP Phone Data Traffic  14-2
- Configuring Voice VLAN  14-3
  - Default Voice VLAN Configuration  14-3
  - Voice VLAN Configuration Guidelines  14-3
  - Configuring a Port Connected to a Cisco 7960 IP Phone  14-4
    - Configuring IP Phone Voice Traffic  14-4
    - Configuring the Priority of Incoming Data Frames  14-5
- Displaying Voice VLAN  14-6

CHAPTER 15
Configuring IEEE 802.1Q and Layer 2 Protocol Tunneling  15-1
- Understanding IEEE 802.1Q Tunneling  15-1
- Configuring IEEE 802.1Q Tunneling  15-4
  - Default IEEE 802.1Q Tunneling Configuration  15-4
  - IEEE 802.1Q Tunneling Configuration Guidelines  15-4
    - Native VLANs  15-4
    - System MTU  15-5
  - IEEE 802.1Q Tunneling and Other Features  15-6
    - Configuring an IEEE 802.1Q Tunneling Port  15-6
- Configuring VLAN Mapping  15-7
  - Default VLAN Mapping Configuration  15-8
  - Mapping Customer VLANs to Service-Provider VLANs  15-8
  - Mapping Customer IEEE 802.1Q Tunnel VLANs to Service-Provider VLANs  15-10
- Configuring IEEE 802.1ad  15-11
Configuring a Secondary Root Switch 16-16
Configuring Port Priority 16-16
Configuring Path Cost 16-18
Configuring the Switch Priority of a VLAN 16-19
Configuring Spanning-Tree Timers 16-20
  Configuring the Hello Time 16-20
  Configuring the Forwarding-Delay Time for a VLAN 16-21
  Configuring the Maximum-Aging Time for a VLAN 16-21
Displaying the Spanning-Tree Status 16-22

CHAPTER 17 Configuring MSTP 17-1
Understanding MSTP 17-2
  Multiple Spanning-Tree Regions 17-2
  IST, CIST, and CST 17-2
    Operations Within an MST Region 17-3
    Operations Between MST Regions 17-4
  IEEE 802.1s Terminology 17-5
  Hop Count 17-5
  Boundary Ports 17-6
  IEEE 802.1s Implementation 17-6
    Port Role Naming Change 17-6
    Interoperation Between Legacy and Standard Switches 17-7
    Detecting Unidirectional Link Failure 17-7
    Interoperability with 802.1D STP 17-8
Understanding RSTP 17-8
  Port Roles and the Active Topology 17-9
  Rapid Convergence 17-9
  Synchronization of Port Roles 17-11
  Bridge Protocol Data Unit Format and Processing 17-11
    Processing Superior BPDU Information 17-12
    Processing Inferior BPDU Information 17-12
  Topology Changes 17-13
Configuring MSTP Features 17-13
  Default MSTP Configuration 17-14
  MSTP Configuration Guidelines 17-14
  Specifying the MST Region Configuration and Enabling MSTP 17-15
  Configuring the Root Switch 17-17
  Configuring a Secondary Root Switch 17-18
  Configuring Port Priority 17-19
Configuring Path Cost 17-20
Configuring the Switch Priority 17-21
Configuring the Hello Time 17-22
Configuring the Forwarding-Delay Time 17-23
Configuring the Maximum-Aging Time 17-23
Configuring the Maximum-Hop Count 17-24
Specifying the Link Type to Ensure Rapid Transitions 17-24
Designating the Neighbor Type 17-25
Restarting the Protocol Migration Process 17-25
Displaying the MST Configuration and Status 17-26

**CHAPTER 18**

Configuring Optional Spanning-Tree Features 18-1
Understanding Optional Spanning-Tree Features 18-1
  Understanding Port Fast 18-2
  Understanding BPDU Guard 18-2
  Understanding BPDU Filtering 18-3
  Understanding UplinkFast 18-3
  Understanding BackboneFast 18-5
  Understanding EtherChannel Guard 18-7
  Understanding Root Guard 18-8
  Understanding Loop Guard 18-9
Configuring Optional Spanning-Tree Features 18-9
  Default Optional Spanning-Tree Configuration 18-9
  Optional Spanning-Tree Configuration Guidelines 18-10
Enabling Port Fast 18-10
Enabling BPDU Guard 18-11
Enabling BPDU Filtering 18-12
Enabling UplinkFast for Use with Redundant Links 18-13
Enabling BackboneFast 18-13
Enabling EtherChannel Guard 18-14
Enabling Root Guard 18-15
Enabling Loop Guard 18-15
Displaying the Spanning-Tree Status 18-16

**CHAPTER 19**

Configuring Resilient Ethernet Protocol 19-1
Understanding REP 19-1
  Link Integrity 19-3
  Fast Convergence 19-4
  VLAN Load Balancing 19-4
Contents

Catalyst 3750 Metro Switch Software Configuration Guide

OL-9644-09

Spanning Tree Interaction 19-6
REP Ports 19-6
Configuring REP 19-7
Default REP Configuration 19-7
REP Configuration Guidelines 19-7
Configuring the REP Administrative VLAN 19-9
Configuring REP Interfaces 19-10
Setting Manual Preemption for VLAN Load Balancing 19-14
Configuring SNMP Traps for REP 19-14
Monitoring REP 19-15

CHAPTER 20
Configuring Flex Links and the MAC Address-Table Move Update Feature 20-1
Understanding Flex Links and the MAC Address-Table Move Update 20-1
Flex Links 20-1
VLAN Flex Link Load Balancing and Support 20-2
Flex Link Multicast Fast Convergence 20-3
Learning the Other Flex Link Port as the mortar Port 20-3
Generating IGMP Reports 20-3
Leaking IGMP Reports 20-4
MAC Address-Table Move Update 20-6
Configuring Flex Links and MAC Address-Table Move Update 20-7
Default Configuration 20-8
Configuration Guidelines 20-8
Configuring Flex Links 20-9
Configuring VLAN Load Balancing on Flex Links 20-11
Configuring the MAC Address-Table Move Update Feature 20-12
Monitoring Flex Links and the MAC Address-Table Move Update 20-14

CHAPTER 21
Configuring DHCP Features and IP Source Guard 21-1
Understanding DHCP Features 21-1
DHCP Server 21-2
DHCP Relay Agent 21-2
DHCP Snooping 21-2
Option-82 Data Insertion 21-3
Cisco IOS DHCP Server Database 21-6
DHCP Snooping Binding Database 21-6
Configuring DHCP Features 21-8
Default DHCP Configuration 21-8
DHCP Snooping Configuration Guidelines 21-9
Configuring the DHCP Server 21-10
Configuring the DHCP Relay Agent 21-10
Specifying the Packet Forwarding Address 21-10
Enabling DHCP Snooping and Option 82 21-11
Enabling DHCP Snooping on Private VLANs 21-13
Enabling the Cisco IOS DHCP Server Database 21-14
Enabling the DHCP Snooping Binding Database Agent 21-14
Displaying DHCP Snooping Information 21-15
Understanding IP Source Guard 21-15
Source IP Address Filtering 21-16
Source IP and MAC Address Filtering 21-16
IP Source Guard for Static Hosts 21-16
Configuring IP Source Guard 21-17
Default IP Source Guard Configuration 21-17
IP Source Guard Configuration Guidelines 21-17
Enabling IP Source Guard 21-18
Configuring IP Source Guard for Static Hosts 21-19
Configuring IP Source Guard for Static Hosts on a Layer 2 Access Port 21-19
Configuring IP Source Guard for Static Hosts on a Private VLAN Host Port 21-23
Displaying IP Source Guard Information 21-25
Understanding DHCP Server Port-Based Address Allocation 21-25
Configuring DHCP Server Port-Based Address Allocation 21-26
Default Port-Based Address Allocation Configuration 21-26
Port-Based Address Allocation Configuration Guidelines 21-26
Enabling DHCP Server Port-Based Address Allocation 21-26
Displaying DHCP Server Port-Based Address Allocation 21-29

CHAPTER 22
Configuring Dynamic ARP Inspection 22-1
Understanding Dynamic ARP Inspection 22-1
Interface Trust States and Network Security 22-3
Rate Limiting of ARP Packets 22-4
Relative Priority of ARP ACLs and DHCP Snooping Entries 22-4
Logging of Dropped Packets 22-4
Configuring Dynamic ARP Inspection 22-5
Default Dynamic ARP Inspection Configuration 22-5
Dynamic ARP Inspection Configuration Guidelines 22-6
Configuring Dynamic ARP Inspection in DHCP Environments 22-7
Configuring ARP ACLs for Non-DHCP Environments 22-8
Limiting the Rate of Incoming ARP Packets 22-10
Performing Validation Checks 22-11
Configuring the Log Buffer 22-12
Displaying Dynamic ARP Inspection Information 22-14

CHAPTER 23
Configuring IGMP Snooping and MVR 23-1
Understanding IGMP Snooping 23-1
  IGMP Versions 23-2
  Joining a Multicast Group 23-3
  Leaving a Multicast Group 23-4
  Immediate Leave 23-5
  IGMP Report Suppression 23-5
Configuring IGMP Snooping 23-5
  Default IGMP Snooping Configuration 23-6
  Enabling or Disabling IGMP Snooping 23-6
  Setting the Snooping Method 23-7
  Configuring a Multicast Router Port 23-8
  Configuring a Host Staticaly to Join a Group 23-9
  Enabling IGMP Immediate Leave 23-10
  Configuring the IGMP Snooping Querier 23-10
  Disabling IGMP Report Suppression 23-12
Displaying IGMP Snooping Information 23-12
Understanding Multicast VLAN Registration 23-13
  Using MVR in a Multicast Television Application 23-14
Configuring MVR 23-16
  Default MVR Configuration 23-16
  MVR Configuration Guidelines and Limitations 23-16
  Configuring MVR Global Parameters 23-17
  Configuring MVR on Access Ports 23-18
  Configuring MVR on Trunk Ports 23-20
Displaying MVR Information 23-21
Configuring IGMP Filtering and Throttling 23-21
  Default IGMP Filtering and Throttling Configuration 23-22
  Configuring IGMP Profiles 23-22
  Applying IGMP Profiles 23-23
  Setting the Maximum Number of IGMP Groups 23-24
  Configuring the IGMP Throttling Action 23-25
  Displaying IGMP Filtering and Throttling Configuration 23-26
CHAPTER 24
Configuring Port-Based Traffic Control 24-1
  Configuring Storm Control 24-1
    Understanding Storm Control 24-1
    Default Storm Control Configuration 24-3
  Configuring Storm Control and Threshold Levels 24-3
  Configuring Small-Frame Arrival Rate 24-5
  Configuring Protected Ports 24-6
    Default Protected Port Configuration 24-6
    Protected Port Configuration Guidelines 24-6
  Configuring a Protected Port 24-7
  Configuring Port Blocking 24-7
    Default Port Blocking Configuration 24-7
    Blocking Flooded Traffic on an Interface 24-8
  Configuring Port Security 24-8
    Understanding Port Security 24-9
    Secure MAC Addresses 24-9
    Security Violations 24-10
    Default Port Security Configuration 24-11
    Configuration Guidelines 24-11
    Enabling and Configuring Port Security 24-12
    Enabling and Configuring Port Security Aging 24-15
    Port Security and Private VLANs 24-16

CHAPTER 25
Configuring CDP 25-1
  Understanding CDP 25-1
  Configuring CDP 25-2
    Default CDP Configuration 25-2
    Configuring the CDP Characteristics 25-2
    Disabling and Enabling CDP 25-3
    Disabling and Enabling CDP on an Interface 25-4
    Monitoring and Maintaining CDP 25-4

CHAPTER 26
Configuring LLDP and LLDP-MED 26-1
  Understanding LLDP and LLDP-MED 26-1
  Understanding LLDP 26-1
  Understanding LLDP-MED 26-2
  Configuring LLDP and LLDP-MED 26-3
  Default LLDP Configuration 26-3
Configuring LLDP Characteristics 26-4
Disabling and Enabling LLDP Globally 26-5
Disabling and Enabling LLDP on an Interface 26-5
Configuring LLDP-MED TLVs 26-6
Monitoring and Maintaining LLDP and LLDP-MED 26-7

CHAPTER 27
Configuring UDLD 27-1
Understanding UDLD 27-1
Modes of Operation 27-1
Methods to Detect Unidirectional Links 27-2
Configuring UDLD 27-4
Default UDLD Configuration 27-4
UDLD Configuration Guidelines 27-4
Enabling UDLD Globally 27-5
Enabling UDLD on an Interface 27-5
Resetting an Interface Disabled by UDLD 27-6
Displaying UDLD Status 27-6

CHAPTER 28
Configuring SPAN and RSPAN 28-1
Understanding SPAN and RSPAN 28-1
Local SPAN 28-2
Remote SPAN 28-2
SPAN and RSPAN Concepts and Terminology 28-3
SPAN Sessions 28-3
Monitored Traffic 28-4
Source Ports 28-5
Source VLANs 28-6
VLAN Filtering 28-6
Destination Port 28-7
RSPAN VLAN 28-8
SPAN and RSPAN Interaction with Other Features 28-8
Configuring SPAN and RSPAN 28-9
Default SPAN and RSPAN Configuration 28-9
Configuring Local SPAN 28-10
SPAN Configuration Guidelines 28-10
Creating a Local SPAN Session 28-11
Creating a Local SPAN Session and Configuring Ingress Traffic 28-13
Specifying VLANs to Filter 28-14
Configuring RSPAN 28-15
RSPAN Configuration Guidelines 28-16
Configuring a VLAN as an RSPAN VLAN 28-16
Creating an RSPAN Source Session 28-17
Creating an RSPAN Destination Session 28-19
Creating an RSPAN Destination Session and Configuring Incoming Traffic 28-20
Specifying VLANs to Filter 28-22
Displaying SPAN and RSPAN Status 28-23

CHAPTER 29
Configuring RMON 29-1
Understanding RMON 29-1
Configuring RMON 29-3
Default RMON Configuration 29-3
Configuring RMON Alarms and Events 29-3
Collecting Group History Statistics on an Interface 29-5
Collecting Group Ethernet Statistics on an Interface 29-6
Displaying RMON Status 29-6

CHAPTER 30
Configuring System Message Logging 30-1
Understanding System Message Logging 30-1
Configuring System Message Logging 30-2
System Log Message Format 30-2
Default System Message Logging Configuration 30-3
Disabling Message Logging 30-4
Setting the Message Display Destination Device 30-4
Synchronizing Log Messages 30-5
Enabling and Disabling Timestamps on Log Messages 30-7
Enabling and Disabling Sequence Numbers in Log Messages 30-7
Defining the Message Severity Level 30-8
Limiting Syslog Messages Sent to the History Table and to SNMP 30-9
Enabling the Configuration-Change Logger 30-10
Configuring UNIX Syslog Servers 30-11
Logging Messages to a UNIX Syslog Daemon 30-11
Configuring the UNIX System Logging Facility 30-12
Displaying the Logging Configuration 30-13

CHAPTER 31
Configuring SNMP 31-1
Understanding SNMP 31-1
SNMP Versions 31-2
SNMP Manager Functions 31-4
SNMP Agent Functions 31-4
SNMP Community Strings 31-4
Using SNMP to Access MIB Variables 31-5
SNMP Notifications 31-5
SNMP ifIndex MIB Object Values 31-6
MIB Data Collection and Transfer 31-6

Configuring SNMP 31-7
Default SNMP Configuration 31-7
SNMP Configuration Guidelines 31-7
Disabling the SNMP Agent 31-8
Configuring Community Strings 31-8
Configuring SNMP Groups and Users 31-10
Configuring SNMP Notifications 31-12
Setting the Agent Contact and Location Information 31-17
Limiting TFTP Servers Used Through SNMP 31-18
Setting the CPU Threshold Notification Types and Values 31-18
Configuring MIB Data Collection and Transfer 31-19
Configuring the Cisco Process MIB CPU Threshold Table 31-22
SNMP Examples 31-23

Displaying SNMP Status 31-24

CHAPTER 32
Configuring Embedded Event Manager 32-1
Understanding Embedded Event Manager 32-1
Event Detectors 32-3
Embedded Event Manager Actions 32-4
Embedded Event Manager Policies 32-4
Embedded Event Manager Environment Variables 32-5
EEM 3.2 32-5

Configuring Embedded Event Manager 32-6
Registering and Defining an Embedded Event Manager Applet 32-6
Registering and Defining an Embedded Event Manager TCL Script 32-7
Displaying Embedded Event Manager Information 32-7

CHAPTER 33
Configuring Network Security with ACLs 33-1
Understanding ACLs 33-1
Supported ACLs 33-2
Router ACLs 33-3
Port ACLs 33-4
VLAN Maps 33-4
Handling Fragmented and Unfragmented Traffic 33-5
Configuring IP ACLs 33-6
  Creating Standard and Extended IP ACLs 33-7
    Access List Numbers 33-7
    Creating a Numbered Standard ACL 33-8
    Creating a Numbered Extended ACL 33-9
    Resequencing ACEs in an ACL 33-14
    Creating Named Standard and Extended ACLs 33-14
  Using Time Ranges with ACLs 33-16
  Including Comments in ACLs 33-18
  Applying an IP ACL to a Terminal Line 33-18
  Applying an IP ACL to an Interface 33-19
  Hardware and Software Treatment of IP ACLs 33-21
Troubleshooting ACLs 33-21
  IP ACL Configuration Examples 33-22
    Numbered ACLs 33-24
    Extended ACLs 33-24
    Named ACLs 33-24
    Time Range Applied to an IP ACL 33-25
    Commented IP ACL Entries 33-25
    ACL Logging 33-26
  Creating Named MAC Extended ACLs 33-27
    Applying a MAC ACL to a Layer 2 Interface 33-28
Configuring VLAN Maps 33-29
  VLAN Map Configuration Guidelines 33-30
  Creating a VLAN Map 33-31
    Examples of ACLs and VLAN Maps 33-32
    Applying a VLAN Map to a VLAN 33-34
    Using VLAN Maps in Your Network 33-34
      Wiring Closet Configuration 33-34
      Denying Access to a Server on Another VLAN 33-35
Using VLAN Maps with Router ACLs 33-36
  Guidelines 33-37
    Examples of Router ACLs and VLAN Maps Applied to VLANs 33-38
      ACLs and Switched Packets 33-38
      ACLs and Bridged Packets 33-38
      ACLs and Routed Packets 33-39
      ACLs and Multicast Packets 33-40
Configuring QoS 34-1

QoS Overview 34-2

Basic QoS Model 34-4
  Supported Policy Maps 34-7
  Supported Policing Configurations 34-8

Understanding Standard QoS 34-9
  Ingress Classification 34-9
    Ingress Classification Based on QoS ACLs 34-11
    Ingress Classification Based on Traffic Classes and Traffic Policies 34-12
  Ingress Policing and Marking 34-13
    Nonhierarchical Single-Level Policing 34-13
    Hierarchical Dual-Level Policing on SVIs 34-15

Mapping Tables 34-17

Queueing and Scheduling Overview 34-17
  Weighted Tail Drop 34-19
  SRR Shaping and Sharing 34-19
  Queueing and Scheduling of Ingress Queues 34-20
  Queueing and Scheduling of Egress Queue-Sets 34-22

QoS Treatment for Performance-Monitoring Protocols 34-25
  Cisco IP-SLAs 34-26
  Two-Way Active Measurement Protocol 34-26
  QoS Treatment for IP-SLA and TWAMP Probes 34-26
    Marking 34-26
    Queuing 34-26
  QoS Marking for CPU-Generated Traffic 34-27
  QoS Queuing for CPU-Generated Traffic 34-28
  Configuration Guidelines 34-29

Understanding Hierarchical QoS 34-30
  Hierarchical Levels 34-30
  Hierarchical Classification Based on Traffic Classes and Traffic Policies 34-33
  Hierarchical Policies and Marking 34-34
  Queueing and Scheduling of Hierarchical Queues 34-37
    Hierarchical Queues 34-38
    Congestion-Management and Congestion-Avoidance Features 34-38
  Hierarchical QoS on EtherChannels 34-40

Configuring Auto-QoS 34-40
  Generated Auto-QoS Configuration 34-41
<table>
<thead>
<tr>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effects of Auto-QoS on the Configuration</td>
</tr>
<tr>
<td>Auto-QoS Configuration Guidelines</td>
</tr>
<tr>
<td>Upgrading from a Previous Software Release</td>
</tr>
<tr>
<td>Enabling Auto-QoS for VoIP</td>
</tr>
<tr>
<td>Auto-QoS Configuration Example</td>
</tr>
<tr>
<td>Displaying Auto-QoS Information</td>
</tr>
<tr>
<td>Configuring Standard QoS</td>
</tr>
<tr>
<td>Standard QoS Configuration</td>
</tr>
<tr>
<td>Ingress Queue Configuration</td>
</tr>
<tr>
<td>Egress Queue-Set Configuration</td>
</tr>
<tr>
<td>Mapping Table Configuration</td>
</tr>
<tr>
<td>Standard QoS Configuration Guidelines</td>
</tr>
<tr>
<td>Packet Modification</td>
</tr>
<tr>
<td>Enabling QoS Globally</td>
</tr>
<tr>
<td>Configuring Ingress Classification by Using Port Trust States</td>
</tr>
<tr>
<td>Configuring the Trust State on Ports Within the QoS Domain</td>
</tr>
<tr>
<td>Configuring the CoS Value for an Interface</td>
</tr>
<tr>
<td>Configuring a Trusted Boundary to Ensure Port Security</td>
</tr>
<tr>
<td>Enabling DSCP Transparency Mode</td>
</tr>
<tr>
<td>Configuring the DSCP Trust State on a Port Bordering Another QoS Domain</td>
</tr>
<tr>
<td>Configuring an Ingress QoS Policy</td>
</tr>
<tr>
<td>Classifying Ingress Traffic by Using ACLs</td>
</tr>
<tr>
<td>Classifying Ingress Traffic by Using Class Maps</td>
</tr>
<tr>
<td>Marking and Queuing CPU-Generated Traffic</td>
</tr>
<tr>
<td>Classifying, Policing, and Marking Ingress Traffic by Using Nonhierarchical Single-Level Policy Maps</td>
</tr>
<tr>
<td>Classifying, Policing, and Marking Traffic by Using Hierarchical Dual-Level Policy Maps</td>
</tr>
<tr>
<td>Classifying, Policing, and Marking Ingress Traffic by Using Aggregate Policers</td>
</tr>
<tr>
<td>Configuring DSCP Maps</td>
</tr>
<tr>
<td>Configuring the CoS-to-DSCP Map</td>
</tr>
<tr>
<td>Configuring the IP-Precedence-to-DSCP Map</td>
</tr>
<tr>
<td>Configuring the Policed-DSCP Map</td>
</tr>
<tr>
<td>Configuring the DSCP-to-CoS Map</td>
</tr>
<tr>
<td>Configuring the DSCP-to-DSCP-Mutation Map</td>
</tr>
<tr>
<td>Configuring Ingress Queue Characteristics</td>
</tr>
<tr>
<td>Mapping DSCP or CoS Values to an Ingress Queue and Setting WTD Thresholds</td>
</tr>
<tr>
<td>Allocating Buffer Space Between the Ingress Queues</td>
</tr>
<tr>
<td>Allocating Bandwidth Between the Ingress Queues</td>
</tr>
<tr>
<td>Configuring the Ingress Priority Queue</td>
</tr>
<tr>
<td>Configuring Egress Queue-Set Characteristics</td>
</tr>
</tbody>
</table>
Contents

Allocating Buffer Space to and Setting WTD Thresholds for an Egress Queue-Set 34-91
Mapping DSCP or CoS Values to an Egress Queue-Set and to a Threshold ID 34-93
Configuring SRR Shaped Weights on an Egress Queue-Set 34-95
Configuring SRR Shared Weights on an Egress Queue-Set 34-96
Configuring the Egress Priority Queue 34-97
Limiting the Egress Bandwidth on a Queue-Set 34-97
Configuring Marking and Queuing for CPU-Generated Traffic 34-98
Displaying Standard QoS Information 34-102
Configuring Hierarchical QoS 34-103
Hierarchical QoS Configuration 34-103
Hierarchical QoS Configuration Guidelines 34-103
Hierarchical QoS Over EtherChannel Configuration Guidelines 34-105
Configuring a Hierarchical QoS Policy 34-107
Classifying Traffic by Using Hierarchical Class Maps 34-108
Configuring a Hierarchical Two-Rate Traffic Policer 34-110
Configuring Class-Based Packet Marking in a Hierarchical Traffic Policy 34-114
Configuring CBWFQ and Tail Drop 34-116
Configuring CBWFQ and DSCP-Based WRED 34-119
Configuring CBWFQ and IP Precedence-Based WRED 34-123
Enabling LLQ 34-127
Configuring Shaping 34-129
Displaying Hierarchical QoS Information 34-131

Chapter 35

Configuring EtherChannels and Link-State Tracking 35-1
Understanding EtherChannels 35-1
EtherChannel Overview 35-2
Port-Channel Interfaces 35-3
Port Aggregation Protocol 35-4
PAgP Modes 35-4
PAgP Interaction with Other Features 35-5
Link Aggregation Control Protocol 35-5
LACP Modes 35-5
LACP Interaction with Other Features 35-6
EtherChannel On Mode 35-6
Load Balancing and Forwarding Methods 35-6
Configuring EtherChannels 35-8
Default EtherChannel Configuration 35-9
EtherChannel Configuration Guidelines 35-9
Configuring Layer 2 EtherChannels 35-10
## Contents

### Configuring Layer 3 EtherChannels
- Creating Port-Channel Logical Interfaces
- Configuring the Physical Interfaces
- Configuring EtherChannel Load Balancing
- Configuring the PAgP Learn Method and Priority
- Configuring LACP Hot-Standby Ports
- Configuring the LACP System Priority
- Configuring the LACP Port Priority
- Displaying EtherChannel, PAgP, and LACP Status

### Configuring Link-State Tracking
- Understanding Link-State Tracking
- Default Link-State Tracking Configuration
- Link-State Tracking Configuration Guidelines
- Configuring Link-State Tracking
- Displaying Link-State Tracking Status

### Configuring IP Unicast Routing
- Understanding IP Routing
- Steps for Configuring Routing
- Configuring IP Addressing
- Default Addressing Configuration
- Assigning IP Addresses to Network Interfaces
- Use of Subnet Zero
- Classless Routing
- Configuring Address Resolution Methods
- Define a Static ARP Cache
- Set ARP Encapsulation
- Enable Proxy ARP
- Routing Assistance When IP Routing is Disabled
- Proxy ARP
- Default Gateway
- ICMP Router Discovery Protocol (IRDP)
- Configuring Broadcast Packet Handling
- Enabling Directed Broadcast-to-Physical Broadcast Translation
- Forwarding UDP Broadcast Packets and Protocols
- Establishing an IP Broadcast Address
- Flooding IP Broadcasts
- Monitoring and Maintaining IP Addressing
- Enabling IP Unicast Routing
Configuring RIP

Default RIP Configuration
Configuring Basic RIP Parameters
Configuring RIP Authentication
Configuring Summary Addresses and Split Horizon
Configuring Split Horizon

Configuring OSPF

Default OSPF Configuration
Nonstop Forwarding Awareness
Configuring Basic OSPF Parameters
Configuring OSPF Interfaces
Configuring OSPF Network Types
 Configuring OSPF for Nonbroadcast Networks
 Configuring Network Types for OSPF Interfaces
Configuring OSPF Area Parameters
Configuring Other OSPF Parameters
Changing LSA Group Pacing
Configuring a Loopback Interface
Monitoring OSPF

Configuring EIGRP

Default EIGRP Configuration
Nonstop Forwarding Awareness
Configuring Basic EIGRP Parameters
Configuring EIGRP Interfaces
Configuring EIGRP Route Authentication
Configuring EIGRP Stub Routing
Monitoring and Maintaining EIGRP

Configuring BGP

Default BGP Configuration
Nonstop Forwarding Awareness
Enabling BGP Routing
Managing Routing Policy Changes
Configuring BGP Decision Attributes
Configuring BGP Filtering with Route Maps
Configuring BGP Filtering by Neighbor
Configuring Prefix Lists for BGP Filtering
Configuring BGP Community Filtering
Configuring BGP Neighbors and Peer Groups
Configuring Aggregate Addresses
Contents

Configuring Routing Domain Confederations 36-60
Configuring BGP Route Reflectors 36-61
Configuring Route Dampening 36-62
Monitoring and Maintaining BGP 36-63
Configuring ISO CLNS Routing 36-64
Configuring IS-IS Dynamic Routing 36-64
  Default IS-IS Configuration 36-65
  Nonstop Forwarding Awareness 36-66
  Enabling IS-IS Routing 36-66
  Configuring IS-IS Global Parameters 36-68
  Configuring IS-IS Interface Parameters 36-70
  Monitoring and Maintaining ISO IGRP and IS-IS 36-72
Configuring BFD 36-73
  Default BFD Configuration 36-75
  BFD Configuration Guidelines 36-76
  Configuring BFD Session Parameters on an Interface 36-77
  Enabling BFD Routing Protocol Clients 36-78
    Configuring BFD for OSPF 36-78
    Configuring BFD for IS-IS 36-79
    Configuring BFD for BGP 36-81
    Configuring BFD for EIGRP 36-81
    Configuring BFD for HSRP 36-82
    Disabling BFD Echo Mode 36-82
Configuring Multi-VRF CE 36-83
  Understanding Multi-VRF CE 36-84
  Default Multi-VRF CE Configuration 36-86
  Multi-VRF CE Configuration Guidelines 36-86
Configuring VRFs 36-88
Configuring VRF-Aware Services 36-88
  User Interface for ARP 36-89
  User Interface for PING 36-89
  User Interface for SNMP 36-89
  User Interface for HSRP 36-90
  User Interface for Syslog 36-90
  User Interface for Traceroute 36-91
  User Interface for FTP and TFTP 36-91
  User Interface for VRF-Aware RADIUS 36-91
Configuring Multicast VRFs 36-92
Configuring a VPN Routing Session 36-92
Configuring BGP PE to CE Routing Sessions 36-93
<table>
<thead>
<tr>
<th>Contents</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-VRF CE Configuration Example</td>
<td>36-94</td>
</tr>
<tr>
<td>Displaying Multi-VRF CE Status</td>
<td>36-97</td>
</tr>
<tr>
<td>Configuring Protocol-Independent Features</td>
<td>36-98</td>
</tr>
<tr>
<td>Configuring Cisco Express Forwarding</td>
<td>36-98</td>
</tr>
<tr>
<td>Configuring the Number of Equal-Cost Routing Paths</td>
<td>36-99</td>
</tr>
<tr>
<td>Configuring Static Unicast Routes</td>
<td>36-100</td>
</tr>
<tr>
<td>Specifying Default Routes and Networks</td>
<td>36-101</td>
</tr>
<tr>
<td>Using Route Maps to Redistribute Routing Information</td>
<td>36-102</td>
</tr>
<tr>
<td>Configuring Policy-Based Routing</td>
<td>36-106</td>
</tr>
<tr>
<td>PBR Configuration Guidelines</td>
<td>36-107</td>
</tr>
<tr>
<td>Enabling PBR</td>
<td>36-107</td>
</tr>
<tr>
<td>Filtering Routing Information</td>
<td>36-109</td>
</tr>
<tr>
<td>Setting Passive Interfaces</td>
<td>36-109</td>
</tr>
<tr>
<td>Controlling Advertising and Processing in Routing Updates</td>
<td>36-110</td>
</tr>
<tr>
<td>Filtering Sources of Routing Information</td>
<td>36-110</td>
</tr>
<tr>
<td>Managing Authentication Keys</td>
<td>36-111</td>
</tr>
<tr>
<td>Monitoring and Maintaining the IP Network</td>
<td>36-112</td>
</tr>
</tbody>
</table>

**CHAPTER 37**

**Configuring IPv6 Unicast Routing** 37-1

- Understanding IPv6 37-1
- IPv6 Addresses 37-2
- Supported IPv6 Unicast Routing Features 37-2
  - 128-Bit Wide Unicast Addresses 37-3
  - DNS for IPv6 37-3
  - Path MTU Discovery for IPv6 Unicast 37-4
  - ICMPv6 37-4
  - Neighbor Discovery 37-4
  - Default Router Preference 37-4
- IPv6 Stateless Autoconfiguration and Duplicate Address Detection 37-4
- IPv6 Applications 37-5
- Dual IPv4 and IPv6 Protocol Stacks 37-5
- DHCP for IPv6 Address Assignment 37-6
- Static Routes for IPv6 37-6
- RIP for IPv6 37-6
- OSPF for IPv6 37-6
- EIGRP for IPv6 37-6
- Multiprotocol BGP for IPv6 37-7
- SNMP and Syslog Over IPv6 37-7
- HTTP(S) Over IPv6 37-7
Unsupported IPv6 Unicast Routing Features 37-8
Limitations 37-8
Configuring IPv6 37-9
  Default IPv6 Configuration 37-9
  Configuring IPv6 Addressing and Enabling IPv6 Routing 37-10
  Configuring Default Router Preference 37-12
  Configuring IPv4 and IPv6 Protocol Stacks 37-12
  Configuring DHCP for IPv6 Address Assignment 37-14
    Default DHCPv6 Address Assignment Configuration 37-14
    DHCPv6 Address Assignment Configuration Guidelines 37-14
    Enabling DHCPv6 Server Function 37-15
    Enabling DHCPv6 Client Function 37-17
  Configuring IPv6 ICMP Rate Limiting 37-17
  Configuring CEF for IPv6 37-18
  Configuring Static Routes for IPv6 37-18
  Configuring RIP for IPv6 37-20
  Configuring OSPF for IPv6 37-21
  Configuring EIGRP for IPv6 37-23
  Configuring BGP for IPv6 37-23
Displaying IPv6 37-24

CHAPTER 38
Configuring IPv6 MLD Snooping 38-1
  Understanding MLD Snooping 38-1
    MLD Messages 38-2
    MLD Queries 38-2
    Multicast Client Aging Robustness 38-3
    Multicast Router Discovery 38-3
    MLD Reports 38-4
    MLD Done Messages and Immediate-Leave 38-4
    Topology Change Notification Processing 38-4
  Configuring IPv6 MLD Snooping 38-5
    Default MLD Snooping Configuration 38-5
    MLD Snooping Configuration Guidelines 38-6
    Enabling or Disabling MLD Snooping 38-6
    Configuring a Static Multicast Group 38-7
    Configuring a Multicast Router Port 38-8
    Enabling MLD Immediate Leave 38-8
    Configuring MLD Snooping Queries 38-9
    Disabling MLD Listener Message Suppression 38-10
CHAPTER 39

Configuring IPv6 ACLs 39-1

Understanding IPv6 ACLs 39-1

Supported ACL Features 39-2
IPv6 ACL Limitations 39-3

Configuring IPv6 ACLs 39-3

Default IPv6 ACL Configuration 39-4
Interaction with Other Features 39-4
Creating IPv6 ACLs 39-4
Applying an IPv6 ACL to an Interface 39-7

Displaying IPv6 ACLs 39-8

CHAPTER 40

Configuring HSRP 40-1

Understanding HSRP 40-1

HSRP Versions 40-3

Configuring HSRP 40-4

Default HSRP Configuration 40-4
HSRP Configuration Guidelines 40-4
Enabling HSRP 40-5
Configuring HSRP Group Attributes 40-6
Configuring HSRP Priority 40-6
Configuring HSRP Authentication and Timers 40-9
Enabling HSRP Support for ICMP Redirect Messages 40-10

Displaying HSRP Configurations 40-10

CHAPTER 41

Configuring Cisco IOS IP SLAs Operations 41-1

Understanding Cisco IOS IP SLAs 41-1

Using Cisco IOS IP SLAs to Measure Network Performance 41-3
IP SLAs Responder and IP SLAs Control Protocol 41-4
Response Time Computation for IP SLAs 41-4
IP SLAs Operation Scheduling 41-5
IP SLAs Operation Threshold Monitoring 41-5

Configuring IP SLAs Operations 41-6

Default Configuration 41-6
Configuration Guidelines 41-6
Configuring the IP SLAs Responder 41-7
Analyzing IP Service Levels by Using the UDP Jitter Operation 41-8

Displaying MLD Snooping Information 38-11
Analyzing IP Service Levels by Using the ICMP Echo Operation 41-11
Monitoring IP SLAs Operations 41-13
Understanding TWAMP 41-14
Configuring TWAMP 41-15
  Configuring the TWAMP Server 41-15
  Configuring the TWAMP Reflector 41-16
Troubleshooting TWAMP 41-16

CHAPTER 42

Configuring Enhanced Object Tracking 42-1
Understanding Enhanced Object Tracking 42-1
Configuring Enhanced Object Tracking Features 42-2
  Default Configuration 42-2
  Tracking Interface Line-Protocol or IP Routing State 42-2
  Configuring a Tracked List 42-3
    Configuring a Tracked List with a Boolean Expression 42-3
    Configuring a Tracked List with a Weight Threshold 42-4
    Configuring a Tracked List with a Percentage Threshold 42-6
  Configuring HSRP Object Tracking 42-7
  Configuring Other Tracking Characteristics 42-8
  Configuring IP SLAs Object Tracking 42-8
  Configuring Static Routing Support 42-10
    Configuring a Primary Interface 42-10
    Configuring a Cisco IP SLAs Monitoring Agent and Track Object 42-11
    Configuring a Routing Policy and Default Route 42-11
Monitoring Enhanced Object Tracking 42-13

CHAPTER 43

Configuring Ethernet OAM, CFM, and E-LMI 43-1
Understanding Ethernet CFM 43-2
  CFM Domain 43-2
  Maintenance Associations and Maintenance Points 43-3
  CFM Messages 43-5
  Crosscheck Function and Static Remote MEPs 43-5
  SNMP Traps and Fault Alarms 43-5
  Configuration Error List 43-6
  CFM Version Interoperability 43-6
  IP SLAs Support for CFM 43-6
Configuring Ethernet CFM 43-7
  Default Ethernet CFM Configuration 43-7
  Ethernet CFM Configuration Guidelines 43-8
Contents

Configuring the CFM Domain 43-8
Configuring Ethernet CFM Crosscheck 43-12
Configuring Static Remote MEP 43-13
Configuring a Port MEP 43-14
Configuring SNMP Traps 43-15
Configuring Fault Alarms 43-16
Configuring IP SLAs CFM Operation 43-17
  Manually Configuring an IP SLAs CFM Probe or Jitter Operation 43-18
  Configuring an IP SLAs Operation with Endpoint Discovery 43-20
Configuring CFM on C-VLAN (Inner VLAN) 43-21
  Feature Support and Behavior 43-22
  Platform Restrictions and Limitations 43-22
Understanding CFM ITU-T Y.1731 Fault Management 43-23
  Y.1731 Terminology 43-23
  Alarm Indication Signals 43-24
  Ethernet Remote Defect Indication 43-24
  Ethernet Locked Signal 43-25
  Multicast Ethernet Loopback 43-25
Configuring Y.1731 Fault Management 43-25
  Default Y.1731 Configuration 43-25
  Configuring ETH-AIS 43-26
  Configuring ETH-LCK 43-27
  Using Multicast Ethernet Loopback 43-30
Managing and Displaying Ethernet CFM Information 43-30
Understanding the Ethernet OAM Protocol 43-32
  OAM Features 43-33
  OAM Messages 43-33
Setting Up and Configuring Ethernet OAM 43-33
  Default Ethernet OAM Configuration 43-34
  Ethernet OAM Configuration Guidelines 43-34
  Enabling Ethernet OAM on an Interface 43-34
  Enabling Ethernet OAM Remote Loopback 43-35
  Configuring Ethernet OAM Link Monitoring 43-36
  Configuring Ethernet OAM Remote Failure Indications 43-39
  Configuring Ethernet OAM Templates 43-39
Displaying Ethernet OAM Protocol Information 43-42
Understanding E-LMI 43-42
  E-LMI Interaction with OAM Manager 43-43
  CFM Interaction with OAM Manager 43-43
Configuring E-LMI 43-44  
- Default E-LMI Configuration 43-44 
- E-LMI and OAM Manager Configuration Guidelines 43-44 
- Configuring the OAM Manager 43-45 
- Enabling E-LMI 43-47 
- Ethernet OAM Manager Configuration Example 43-48 
  - Provider-Edge Device Configuration 43-48 
  - Customer-Edge Device Configuration 43-49 
- Displaying E-LMI and OAM Manager Information 43-49 
- Ethernet CFM and Ethernet OAM Interaction 43-50 
  - Configuring Ethernet OAM Interaction with CFM 43-51 
  - Configuring the OAM Manager 43-51 
  - Enabling Ethernet OAM 43-52 
- Ethernet OAM and CFM Configuration Example 43-52

CHAPTER 44 Configuring MPLS, MPLS VPN, MPLS OAM, and EoMPLS 44-1

- Understanding MPLS Services 44-2 
- Understanding MPLS VPNs 44-3 
  - VPN Benefits 44-4 
  - Distribution of VPN Routing Information 44-6 
- Configuring MPLS VPNs 44-6 
  - Default MPLS Configuration 44-7 
  - MPLS VPN Configuration Guidelines 44-7 
  - Enabling MPLS 44-7 
  - Defining VPNs 44-8 
  - Configuring BGP Routing Sessions 44-9 
  - Configuring Provide-Edge-to-Provider-Edge Routing Sessions 44-10 
  - Configuring BGP Provider-Edge-to-Customer-Edge Routing Sessions 44-10 
  - Configuring RIP Provider-Edge-to-Customer-Edge Routing Sessions 44-11 
  - Configuring Static Route Provider-Edge-to-Customer-Edge Routing Sessions 44-11 
  - Packet Flow in an MPLS VPN 44-12 
- Understanding MPLS Traffic Engineering and Fast Reroute 44-13 
  - MPLS TE 44-13 
  - MPLS TE Fast Reroute 44-14 
  - MPLS TE Primary and Backup Autotunnel 44-15 
- Configuring MPLS Traffic Engineering and Fast Reroute 44-15 
  - Default MPLS TE and Fast Reroute Configuration 44-15 
  - MPLS TE and Fast Reroute Configuration Guidelines 44-15 
  - Configuring MPLS TE 44-16
Configuring an MPLS TE Tunnel 44-16
Configuring the Routing Protocol for MPLS TE 44-17
Configuring TE Fast Reroute 44-18
Configuring a Protected Link to Use a Backup Tunnel 44-19
Configuring Fast Reroute Failure Detection 44-19
Configuring Primary and Backup Autotunnels 44-20
Understanding MPLS OAM 44-21
LSP Ping 44-23
LSP Traceroute 44-23
AToM VCCV (LSP Ping over Pseudowire) 44-24
IP SLAs Interworking with MPLS OAM 44-24
LSP Tree Trace and IP SLAs ECMP Tree Trace 44-24
Configuring MPLS OAM and IP SLAs MPLS 44-25
Default MPLS OAM Configuration 44-25
MPLS OAM Configuration Guidelines 44-25
Using LSP Ping for LDP IPv4 FEC 44-26
Using LSP Traceroute for LDP IPv4 FEC 44-28
Using LSP Ping for Pseudowire (AToM VCCV) 44-29
Configuring IP SLAs MPLS Ping and Traceroute 44-30
Configuring the IP SLAs LSP Health Monitor 44-31
Manually Configuring IP SLAs MPLS LSP Ping or Traceroute 44-34
Using LSP Tree Trace 44-36
Manually Setting LSP Tree Trace 44-36
Configuring ECMP IP SLAs Tree Trace 44-37
Understanding EoMPLS 44-40
Interaction with Other Features 44-41
EoMPLS and IEEE 802.1Q Tunneling 44-41
EoMPLS and Layer 2 Tunneling 44-42
EoMPLS and QoS 44-42
EoMPLS Limitations 44-42
Enabling EoMPLS 44-43
Default EoMPLS Configuration 44-43
EoMPLS Configuration Guidelines 44-43
Configuring EoMPLS 44-44
Packet Flow in an EoMPLS Network 44-45
Configuring L2VPN Pseudowire Redundancy 44-46
Configuration Guidelines 44-47
Configuring the Pseudowire 44-48
Configuring L2VPN Interworking 44-48
Configuring Pseudowire Redundancy 44-49
Forcing a Manual Switchover to the Backup Pseudowire VC 44-50
Monitoring L2VPN Pseudowire Redundancy 44-51
Configuring MPLS and EoMPLS QoS 44-51
Understanding MPLS QoS 44-51
Enabling MPLS and EoMPLS QoS 44-53
Default MPLS and EoMPLS QoS Configuration 44-53
Setting the Priority of Packets with Experimental Bits 44-53
Configuring MPLS VPN QoS 44-55
Monitoring and Maintaining MPLS and EoMPLS 44-55

CHAPTER 45
Configuring IP Multicast Routing 45-1
Understanding Cisco’s Implementation of IP Multicast Routing 45-1
Understanding IGMP 45-2
IGMP Version 1 45-3
IGMP Version 2 45-3
Understanding PIM 45-3
PIM Versions 45-4
PIM Modes 45-4
PIM Stub Routing 45-5
IGMP Helper 45-6
Auto-RP 45-6
Bootstrap Router 45-7
Multicast Forwarding and Reverse Path Check 45-7
Understanding DVMRP 45-8
Understanding CGMP 45-9
Configuring IP Multicast Routing 45-9
Default Multicast Routing Configuration 45-10
Multicast Routing Configuration Guidelines 45-10
PIMv1 and PIMv2 Interoperability 45-10
Auto-RP and BSR Configuration Guidelines 45-11
Configuring Basic Multicast Routing 45-11
Configuring PIM Stub Routing 45-13
PIM Stub Routing Configuration Guidelines 45-13
Enabling PIM Stub Routing 45-13
Configuring Source-Specific Multicast 45-14
SSM Components Overview 45-15
How SSM Differs from Internet Standard Multicast 45-15
SSM IP Address Range 45-15
Contents

SSM Operations 45-15
IGMPv3 Host Signalling 45-16
Configuration Guidelines 45-16
Configuring SSM 45-17
Monitoring SSM 45-17
Configuring Source Specific Multicast Mapping 45-18
   Configuration Guidelines 45-18
   SSM Mapping Overview 45-18
   Configuring SSM Mapping 45-20
   Monitoring SSM Mapping 45-23
Configuring a Rendezvous Point 45-23
   Manually Assigning an RP to Multicast Groups 45-23
   Configuring Auto-RP 45-25
   Configuring PIMv2 BSR 45-29
Using Auto-RP and a BSR 45-33
Monitoring the RP Mapping Information 45-34
Troubleshooting PIMv1 and PIMv2 Interoperability Problems 45-34
Configuring Advanced PIM Features 45-34
   Understanding PIM Shared Tree and Source Tree 45-34
   Delaying the Use of PIM Shortest-Path Tree 45-36
   Modifying the PIM Router-Query Message Interval 45-37
Configuring Optional IGMP Features 45-38
   Default IGMP Configuration 45-38
   Configuring the Switch as a Member of a Group 45-38
   Controlling Access to IP Multicast Groups 45-39
   Changing the IGMP Version 45-40
   Modifying the IGMP Host-Query Message Interval 45-41
   Changing the IGMP Query Timeout for IGMPv2 45-42
   Changing the Maximum Query Response Time for IGMPv2 45-42
   Configuring the Switch as a Statically Connected Member 45-43
Configuring Optional Multicast Routing Features 45-43
   Enabling CGMP Server Support 45-44
   Configuring sdr Listener Support 45-45
      Enabling sdr Listener Support 45-45
      Limiting How Long an sdr Cache Entry Exists 45-45
   Configuring an IP Multicast Boundary 45-46
Configuring Basic DVMRP Interoperability Features 45-48
   Configuring DVMRP Interoperability 45-48
   Configuring a DVMRP Tunnel 45-50
Advertise DVMRP Network 0.0.0.0 to DVMRP Neighbors 45-52
Responding to mrinfo Requests 45-53
Configuring Advanced DVMRP Interoperability Features 45-53
Enabling DVMRP Unicast Routing 45-54
Rejecting a DVMRP Nonpruning Neighbor 45-54
Controlling Route Exchanges 45-57
Limiting the Number of DVMRP Routes Advertised 45-57
Changing the DVMRP Route Threshold 45-57
Configuring a DVMRP Summary Address 45-58
Disabling DVMRP Autosummarization 45-60
Adding a Metric Offset to the DVMRP Route 45-60
Monitoring and Maintaining IP Multicast Routing 45-61
Clearing Caches, Tables, and Databases 45-61
Displaying System and Network Statistics 45-62
Monitoring IP Multicast Routing 45-63

CHAPTER 46
Configuring MSDP 46-1
Understanding MSDP 46-1
MSDP Operation 46-2
MSDP Benefits 46-3
Configuring MSDP 46-3
Default MSDP Configuration 46-4
Configuring a Default MSDP Peer 46-4
Caching Source-Active State 46-6
Requesting Source Information from an MSDP Peer 46-8
Controlling Source Information that Your Switch Originates 46-8
Redistributing Sources 46-9
Filtering Source-Active Request Messages 46-10
Controlling Source Information that Your Switch Forwards 46-11
Using a Filter 46-11
Using TTL to Limit the Multicast Data Sent in SA Messages 46-13
Controlling Source Information that Your Switch Receives 46-13
Configuring an MSDP Mesh Group 46-15
Shutting Down an MSDP Peer 46-15
Including a Bordering PIM Dense-Mode Region in MSDP 46-16
Configuring an Originating Address other than the RP Address 46-17
Monitoring and Maintaining MSDP 46-17
CHAPTER 47

Configuring Fallback Bridging 47-1
Understanding Fallback Bridging 47-1
Configuring Fallback Bridging 47-2
Default Fallback Bridging Configuration 47-3
Fallback Bridging Configuration Guidelines 47-3
Creating a Bridge Group 47-3
Adjusting Spanning-Tree Parameters 47-5
Changing the VLAN-Bridge Spanning-Tree Priority 47-5
Changing the Interface Priority 47-6
Assigning a Path Cost 47-7
Adjusting BPDU Intervals 47-7
Disabling the Spanning Tree on an Interface 47-9
Monitoring and Maintaining Fallback Bridging 47-10

CHAPTER 48

Troubleshooting 48-1
Recovering from Corrupted Software By Using the XMODEM Protocol 48-2
Recovering from a Lost or Forgotten Password 48-3
Procedure with Password Recovery Enabled 48-4
Procedure with Password Recovery Disabled 48-5
Preventing Autonegotiation Mismatches 48-7
SFP Module Security and Identification 48-7
Monitoring SFP Module Status 48-8
Using Ping 48-8
Understanding Ping 48-8
Executing Ping 48-8
Using Layer 2 Traceroute 48-9
Understanding Layer 2 Traceroute 48-10
Usage Guidelines 48-10
Displaying the Physical Path 48-11
Using IP Traceroute 48-11
Understanding IP Traceroute 48-11
Executing IP Traceroute 48-12
Using Debug Commands 48-13
Enabling Debugging on a Specific Feature 48-13
Enabling All-System Diagnostics 48-14
Redirecting Debug and Error Message Output 48-14
Using the show platform forward Command 48-14
Using the crashinfo File 48-17
Clearing the Startup Configuration File  B-18
Deleting a Stored Configuration File  B-18
Replacing and Rolling Back Configurations  B-18
Understanding Configuration Replacement and Rollback  B-18
Configuration Guidelines  B-19
Configuring the Configuration Archive  B-20
Performing a Configuration Replacement or Rollback Operation  B-21

Working with Software Images  B-22
Image Location on the Switch  B-22
tar File Format of Images on a Server or Cisco.com  B-23
Copying Image Files By Using TFTP  B-23
Preparing to Download or Upload an Image File By Using TFTP  B-24
Downloading an Image File By Using TFTP  B-25
Uploading an Image File By Using TFTP  B-26
Copying Image Files By Using FTP  B-26
Preparing to Download or Upload an Image File By Using FTP  B-27
Downloading an Image File By Using FTP  B-28
Uploading an Image File By Using FTP  B-30
Copying Image Files By Using RCP  B-31
Preparing to Download or Upload an Image File By Using RCP  B-31
Downloading an Image File By Using RCP  B-32
Uploading an Image File By Using RCP  B-34

APPENDIX C

Unsupported Commands in Cisco IOS Release 12.2(55)SE  C-1
Access Control Lists  C-1
Unsupported Privileged EXEC Commands  C-1
Unsupported Global Configuration Commands  C-1
ARP  C-1
Unsupported Global Configuration Commands  C-1
Unsupported Interface Configuration Commands  C-2
Boot Loader Commands  C-2
Unsupported User EXEC Command  C-2
Unsupported Global Configuration Command  C-2
CGMP  C-2
Unsupported Privileged EXEC Command  C-2
Unsupported Interface Configuration Commands  C-2
Clustering  C-3
Unsupported Global Configuration Command  C-3
Unsupported Privileged EXEC Commands  C-3
MPLS C-12
  Unsupported Privileged EXEC or User EXEC Commands C-12
  Unsupported Global Configuration Commands C-12
  Unsupported Interface Configuration Commands C-12

  **Physical Interfaces** C-12

  **Tunnel Interfaces** C-12

  Unsupported Routing Commands C-13

MSDP C-13
  Unsupported Privileged EXEC Commands C-13
  Unsupported Global Configuration Commands C-13

QoS C-13
  Unsupported Policy-Map Configuration Command C-13

RADIUS C-13
  Unsupported Global Configuration Commands C-13

SNMP C-14
  Unsupported Global Configuration Commands C-14

Spanning Tree C-14
  Unsupported Global Configuration Commands C-14
  Unsupported Interface Configuration Command C-14

Virtual Forwarding Infrastructure (VFI) C-14
  Unsupported Global Configuration Commands C-14
  Unsupported Privileged EXEC Commands C-14

VLAN C-15
  Unsupported vlan-config Command C-15
  Unsupported Privileged EXEC Command C-15
  Unsupported User EXEC Command C-15

VTP C-15
  Unsupported Privileged EXEC Command C-15
Preface

Audience

This guide is for the networking professional managing the Catalyst 3750 Metro switch, hereafter referred to as the switch. Before using this guide, you should have experience working with the Cisco IOS software and be familiar with the concepts and terminology of Ethernet and local area networking.

Purpose

The Catalyst 3750 Metro switch supports a set of service-provider features, including multiprotocol label switching (MPLS), Ethernet over MPLS (EoMPLS), hierarchical QoS, 802.1Q tunneling, and VLAN mapping. It also supports Layer 2+ features such as access control lists (ACLs) and quality of service (QoS) and Layer 3 features such as IP unicast routing, IP multicast routing, and fallback bridging.

This guide provides procedures for using the commands that have been created or changed for use with the switch. It does not provide detailed information about these commands. For detailed information about these commands, see the Catalyst 3750 Metro Switch Command Reference for this release. For information about the standard Cisco IOS Release 12.2 commands, see the Cisco IOS documentation set available from the Cisco.com home page at Service and Support > Technical Documents. On the Cisco Product Documentation home page, select Release 12.2 from the Cisco IOS Software drop-down list.

This guide does not describe system messages you might encounter or how to install your switch. For more information, see the Catalyst 3750 Metro Switch System Message Guide for this release and to the Catalyst 3750 Metro Switch Hardware Installation Guide.

For documentation updates, see the release notes for this release.

Conventions

This publication uses these conventions to convey instructions and information:

Command descriptions use these conventions:

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

Interactive examples use these conventions:

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

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

<table>
<thead>
<tr>
<th>Note</th>
<th>Means <strong>reader take note</strong>. Notes contain helpful suggestions or references to materials not contained in this manual.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Caution</td>
<td>Means <strong>reader be careful</strong>. In this situation, you might do something that could result in equipment damage or loss of data.</td>
</tr>
</tbody>
</table>

**Related Publications**

These documents provide complete information about the switch and are available from this Cisco.com site:


<table>
<thead>
<tr>
<th>Note</th>
<th>Before installing, configuring, or upgrading the switch, see these documents:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• For initial configuration information, see the “Using Express Setup” chapter or the “Configuring the Switch with the CLI-Based Setup Program” appendix in the hardware installation guide.</td>
</tr>
<tr>
<td></td>
<td>• For upgrade information, see the “Downloading Software” section in the release notes.</td>
</tr>
</tbody>
</table>

• *Release Notes for the Catalyst 3750 Metro Switch*
• *Catalyst 3750 Metro Switch Software Configuration Guide*
• *Catalyst 3750 Metro Switch Command Reference*
• *Catalyst 3750 Metro Switch System Message Guide*
• *Catalyst 3750 Metro Switch Hardware Installation Guide*
• *Cisco Small Form-Factor Pluggable Modules Installation Notes*

• These compatibility matrix documents are available from this Cisco.com site:

  • *Cisco Gigabit Ethernet Transceiver Modules Compatibility Matrix*
  • *Cisco 100-Megabit Ethernet SFP Modules Compatibility Matrix*
  • *Cisco Small Form-Factor Pluggable Modules Compatibility Matrix*
  • *Compatibility Matrix for 1000BASE-T Small Form-Factor Pluggable Modules*
Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What’s New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:


Subscribe to the What’s New in Cisco Product Documentation as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.
Overview

This chapter provides this information about Catalyst 3750 Metro switch software:

- Features, page 1-1
- Default Settings After Initial Switch Configuration, page 1-12
- Network Configuration Examples, page 1-14
- Where to Go Next, page 1-18

Features

Note

Some features noted in this chapter are available only on the cryptographic (that is, supports encryption) versions of the switch software image. You must obtain authorization to use this feature and to download the cryptographic version of the software from Cisco.com. For more information, see the release notes for this release.

Catalyst 3750 Metro switches have these features:

- Performance Features, page 1-2
- Management Options, page 1-3
- Manageability Features, page 1-3 (includes a feature requiring the cryptographic version of the switch software image)
- Availability Features, page 1-4
- VLAN Features, page 1-6
- Layer 2 Virtual Private Network (VPN) Services, page 1-6
- Layer 3 VPN Services, page 1-7
- Security Features, page 1-7 (includes a feature requiring the cryptographic version of the switch software image)
- QoS Features, page 1-8
- Layer 3 Features, page 1-10
- Monitoring Features, page 1-11
Performance Features

- Autosensing of port speed and autonegotiation of duplex mode on all switch ports for optimizing bandwidth
- Automatic-medium-dependent interface crossover (Auto-MDIX) capability on 10/100 Mbps interfaces and 10/100/1000 BASE-T/TX small form-factor pluggable (SFP) interfaces that enables the interface to automatically detect the required cable connection type (straight-through or crossover) and configure the connection appropriately
- Support for up to 1546 bytes for routed frames, up to 9000 bytes for frames that are bridged in hardware, and up to 2000 bytes for frames that are bridged by software
- IEEE 802.3x flow control on all ports (the switch does not send pause frames)
- EtherChannel for enhanced fault tolerance and for providing up to 2 Gbps (Gigabit EtherChannel) or 800 Mbps (Fast EtherChannel) full duplex of bandwidth between switches, routers, and servers
- Port Aggregation Protocol (PAgP) and Link Aggregation Control Protocol (LACP) for automatic creation of EtherChannel links
- Per-port storm control for preventing broadcast, multicast, and unicast storms
- Port blocking on forwarding unknown Layer 2 unknown unicast, multicast, and bridged broadcast traffic
- Cisco Group Management Protocol (CGMP) server support and Internet Group Management Protocol (IGMP) snooping for IGMP Versions 1, 2, and 3:
  - (For CGMP devices) CGMP for limiting multicast traffic to specified end stations and reducing overall network traffic
  - (For IGMP devices) IGMP snooping for efficiently forwarding multimedia and multicast traffic
- Multicast VLAN registration (MVR) to continuously send multicast streams in a multicast VLAN while isolating the streams from subscriber VLANs for bandwidth and security reasons
- MVR over trunk port (MVRoT) support to allow you to configure a trunk port as an MVR receiver port
- IGMP filtering for controlling the set of multicast groups to which hosts on a switch port can belong
- IGMP helper to allow the switch to forward a host request to join a multicast stream to a specific IP destination address
- IGMP throttling for configuring the action when the maximum number of entries is in the IGMP forwarding table
- IGMP report suppression for sending only one IGMP report per multicast router query to the multicast devices (supported only for IGMPv1 or IGMPv2 queries)
- Switch Database Management (SDM) templates for allocating system resources to maximize support for user-selected features
- Configurable small-frame arrival threshold to prevent storm control when small frames (64 bytes or less) arrive on an interface at a specified rate (the threshold)
- RADIUS server load balancing to allow access and authentication requests to be distributed evenly across a server group.
- Multicast VLAN registration (MVR) enhancements include the ability to configure 2000 MVR groups when the switch is in dynamic MVR mode and a new command (mvr ringmode flood) to ensure that forwarding in a ring topology is limited to member ports.
- Support for configuration of an alternate MTU value to allow specific interfaces a different MTU than the global system MTU or jumbo MTU

### Management Options

- **CLI**—The Cisco IOS command-line interface (CLI) software is enhanced to support the Catalyst 3750 Metro switch features. You can access the CLI either by connecting your management station directly to the switch console port or by using Telnet from a remote management station. For more information about the CLI, see Chapter 2, “Using the Command-Line Interface.”
- **CNS**—Cisco Configuration Engine is network management software that acts as a configuration service for automating the deployment and management of network devices and services. You can automate initial configurations and configuration updates by generating switch-specific configuration changes, sending them to the switch, executing the configuration change, and logging the results.
  
  For more information about CNS, see Chapter 4, “Configuring Cisco IOS Configuration Engine.”
- **SNMP**—Simple Network Management Protocol (SNMP) management applications such as CiscoWorks2000 LAN Management Suite (LMS) and HP OpenView. You can manage from an SNMP-compatible management station that is running platforms such as HP OpenView or SunNet Manager. The switch supports a comprehensive set of MIB extensions and four remote monitoring (RMON) groups. You can also use the CLI to configure collection and transfer of selected MIB data or to configure a Cisco Process MIB CPU threshold table. For more information about using SNMP, see Chapter 31, “Configuring SNMP.”

### Manageability Features

**Note**

The encrypted Secure Shell (SSH) feature listed in this section is available only on the cryptographic version of the switch software image.

- Cisco IE2100 Series CNS embedded agents for automating switch management, configuration storage, and delivery
- DHCP for automating configuration of switch information (such as IP address, default gateway, hostname, and Domain Name System [DNS] and TFTP server names)
- DHCP relay agent information (option 82) for subscriber identification and IP address management
- DHCP server for automatic assignment of IP addresses and other DHCP options to IP hosts
- DHCP server port-based address allocation for the preassignment of an IP address to a switch port
- Directed unicast requests to a DNS server for identifying a switch through its IP address and its corresponding hostname and to a TFTP server for administering software upgrades from a TFTP server
- Support for downloading a software image by using a web browser (HTTP).
- Address Resolution Protocol (ARP) for identifying a switch through its IP address and its corresponding MAC address
- Unicast MAC address filtering to drop packets with specific source or destination MAC addresses
- Configurable MAC address scaling that allows disabling MAC address learning on a VLAN to limit the size of the MAC address table
• Cisco Discovery Protocol (CDP) Versions 1 and 2 for network topology discovery and mapping between the switch and other Cisco devices on the network
• Link Layer Discovery Protocol (LLDP) and LLDP Media Endpoint Discovery (LLDP-MED) for interoperability with third-party IP phones
• CDP and LLDP enhancements for exchanging location information with video endpoints for dynamic location-based content distribution from servers
• Network Time Protocol (NTP) for providing a consistent timestamp to all switches from an external source
• Cisco IOS File System (IFS) for providing a single interface to all file systems that the switch uses
• In-band management access for up to 16 simultaneous Telnet connections for multiple CLI-based sessions over the network
• In-band management access for up to five simultaneous, encrypted SSH connections for multiple CLI-based sessions over the network (requires the cryptographic version of the switch software image)
• In-band management access through SNMP Versions 1 and 2, and 3 get and set requests
• Out-of-band management access through the switch console port to a directly attached terminal or to a remote terminal through a serial connection or a modem
• Support for metro Ethernet operation, administration, and maintenance (OAM) IEEE 802.1ag Connectivity Fault Management (CFM), Ethernet Line Management Interface (E-LMI) on customer-edge and provider-edge switches, and IEEE 802.3ah Ethernet OAM discovery, link monitoring, remote fault detection, and remote loopback
• CFM support on a customer VLAN (C-VLAN), which allows a customer to provision maintenance intermediate points (MIPs) and Up maintenance endpoints (MEPs) on a C-VLAN component to provide a customer with visibility to network traffic on the C-VLAN
• Support for the IEEE CFM (IEEE 802.1ap) MIB, which can be used as a tool to trace paths, to verify and to manage connectivity, and to detect faults in a network
• DHCP-based autoconfiguration and image update to download a specified configuration a new image to a large number of switches
• Source Specific Multicast (SSM) mapping for multicast applications to provide a mapping of source to allowing IGMPv2 clients to utilize SSM, allowing listeners to connect to multicast sources dynamically and reducing dependencies on the application
• CPU utilization threshold trap monitors CPU utilization.
• LLDP-MED network-policy profile time, length, value (TLV) for creating a profile for voice and voice-signalling by specifying the values for VLAN, class of service (CoS), differentiated services code point (DSCP), and tagging mode
• Support for including a hostname in the option 12 field of DHCPDISCOVER packets. This provides identical configuration files to be sent by using the DHCP protocol.
• DHCP Snooping enhancement to support the selection of a fixed string-based format for the circuit-id sub-option of the Option 82 DHCP field.

Availability Features

• HSRP for command switch and Layer 3 router redundancy
Chapter 1  Overview

Features

- UniDirectional Link Detection (UDLD) and aggressive UDLD for detecting and disabling unidirectional links on fiber-optic interfaces caused by incorrect fiber-optic wiring or port faults
- IEEE 802.1D Spanning Tree Protocol (STP) for redundant backbone connections and loop-free networks. STP has these features:
  - Up to 128 spanning-tree instances supported
  - Per-VLAN spanning-tree plus (PVST+) for balancing load across VLANs
  - Rapid PVST+ for balancing load across VLANs and providing rapid convergence of spanning-tree instances
  - UplinkFast and BackboneFast for fast convergence after a spanning-tree topology change and for achieving load balancing between redundant uplinks, including Gigabit uplinks
- IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) for grouping VLANs into a spanning-tree instance and for providing multiple forwarding paths for data traffic and load balancing and rapid per-VLAN Spanning-Tree plus (rapid-PVST+) based on the IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) for rapid convergence of the spanning tree by immediately transitioning root and designated ports to the forwarding state
- Optional spanning-tree features available in PVST+, rapid-PVST+, and MSTP mode:
  - Port Fast for eliminating the forwarding delay by enabling a port to immediately transition from the blocking state to the forwarding state
  - BPDU guard for shutting down Port Fast-enabled ports that receive bridge protocol data units (BPDUs)
  - BPDU filtering for preventing a Port Fast-enabled port from sending or receiving BPDUs
  - Root guard for preventing switches outside the network core from becoming the spanning-tree root
  - Loop guard for preventing alternate or root ports from becoming designated ports because of a failure that leads to a unidirectional link
- Equal-cost routing for link-level and switch-level redundancy
- Flex Link Layer 2 interfaces to back up one another as an alternative to STP for basic link redundancy.
- Flex Link Multicast Fast Convergence to reduce the multicast traffic convergence time after a Flex Link failure.
- Link-state tracking to mirror the state of the ports that carry upstream traffic from connected hosts, servers, and other downstream devices. This feature allows the failover of the downstream traffic to an operational link on another Cisco Ethernet switch.
- Support for Resilient Ethernet Protocol (REP) for improved convergence times and network loop prevention without the use of spanning tree
- Counter and timer enhancements to REP support
- REP configuration on edge ports connected to other devices that do not support REP
- Shorter Resilient Ethernet Protocol (REP) hello: Changes the range of the REP link status layer (LSL) age timer from 3000 to 10000 ms in 500-ms intervals to 120 to 10000 ms in 40-ms intervals.
VLAN Features

- Support for up to 1005 VLANs for assigning users to VLANs associated with appropriate network resources, traffic patterns, and bandwidth
- Support for VLAN IDs in the full 1 to 4094 range as allowed by the IEEE 802.1Q standard
- VLAN Query Protocol (VQP) for dynamic VLAN membership
- Inter-Switch Link (ISL) and IEEE 802.1Q trunking encapsulation on all ports for network moves, adds, and changes; management and control of broadcast and multicast traffic; and network security by establishing VLAN groups for high-security users and network resources
- Dynamic Trunking Protocol (DTP) for negotiating trunking on a link between two devices and for negotiating the type of trunking encapsulation (802.1Q or ISL) to be used
- VLAN Trunking Protocol (VTP) and VTP pruning for reducing network traffic by restricting flooded traffic to links destined for stations receiving the traffic
- Voice VLAN for creating subnets for voice traffic from Cisco IP Phones
- VLAN 1 minimization for reducing the risk of spanning-tree loops or storms by allowing VLAN 1 to be disabled on any individual VLAN trunk link. With this feature enabled, no user traffic is sent or received on the trunk, but the switch CPU continues to send and receive control protocol frames.
- Private VLANs to address VLAN scalability problems, to provide a more controlled IP address allocation, and to allow Layer 2 ports to be isolated from other ports on the switch
- VLAN mapping on enhanced-services (ES) ports to translate customer VLANs to service-provider VLANs for transporting packets across the service-provider network without affecting the customer VLAN IDs
- Custom ethertype to enable the user to change the ethertype value on a port to any value to direct the tagged and untagged traffic to different VLANs (ES ports only)
- Port security on a PVLAN host to limit the number of MAC addresses learned on a port, or define which MAC addresses may be learned on a port
- VLAN Flex Link Load Balancing to provide Layer 2 redundancy without requiring Spanning Tree Protocol (STP). A pair of interfaces configured as primary and backup links can load balance traffic based on VLAN.

Layer 2 Virtual Private Network (VPN) Services

- 802.1Q tunneling so that customers with users at remote sites across a service-provider network can keep VLANs segregated from other customers, and Layer 2 protocol tunneling on trunk, access, or tunnel ports to ensure that the customer’s network has complete STP, CDP, and VTP information about all users
- Layer 2 point-to-point tunneling to facilitate the automatic creation of EtherChannels
- Layer 2 protocol tunneling bypass feature to provide interoperability with third-party vendors
- Intelligent 802.1Q tunneling QoS, the ability to copy the inner cost-of-service (CoS) value to the outer CoS value for 802.1Q tunneling
- Support for Ethernet over multiprotocol layer switching (EoMPLS) tunneling mechanism for transporting Ethernet frames over a service-provider MPLS network
- Support for Layer 2 transport over MPLS interworking for Ethernet and VLAN interworking.
• Support for the IEEE 802.1ad standard to provide VLAN scalability in provider networks, giving provider bridges the same functionality as Layer 2 protocol tunneling (L2PT) and QinQ bridges.

Layer 3 VPN Services

• Support for MPLS VPNs provides the capability to deploy and administer scalable Layer 3 VPN services to business customers. Each VPN is associated with one or more VPN routing/forwarding (VRF) instances that include routing and forwarding tables and rules that define the VPN membership. (MPLS VPNs are supported only on ES ports.)
• Support for MPLS Operations, Administration, and Maintenance (OAM) functionality for monitoring lab switched paths (LSPs) and isolating MPLS forwarding problems.
• Multiple VPN multi-VRF instances in customer edge (CE) devices to allow service providers to support multiple VPNs and to overlap IP addresses between VPNs.
• Pseudowire redundancy to allow service providers to configure their multiprotocol label switching (MPLS) networks to detect network failures and to reroute Layer 2 services to another endpoint.
• Support for MPLS traffic engineering and fast reroute link protection for rerouting LSP traffic around a failed link.

Security Features

The Kerberos feature listed in this section is available only on the cryptographic version of the switch software image.

• Password-protected access (read-only and read-write access) to management interfaces for protection against unauthorized configuration changes
• Multilevel security for a choice of security level, notification, and resulting actions
• Static MAC addressing for ensuring security
• Protected port option for restricting the forwarding of traffic to designated ports on the same switch
• Port security option for limiting and identifying MAC addresses of the stations allowed to access the port
• Port security aging to set the aging time for secure addresses on a port
• BPDU guard for shutting down a Port Fast-configured port when an invalid configuration occurs
• Standard and extended IP access control lists (ACLs) for defining security policies in both directions on routed interfaces (router ACLs) and VLANs and inbound on Layer 2 interfaces (port ACLs)
• Extended MAC access control lists for defining security policies in the inbound direction on Layer 2 interfaces
• VLAN ACLs (VLAN maps) for providing intra-VLAN security by filtering traffic based on information in the MAC, IP, and TCP/User Datagram Protocol (UDP) headers
• Source and destination MAC-based ACLs for filtering non-IP traffic
• IEEE 802.1x port-based authentication to prevent unauthorized devices (clients) from gaining access to the network
- IEEE 802.1x with VLAN assignment for restricting 802.1x-authenticated users to a specified VLAN
- IEEE 802.1x with port security for controlling access to 802.1x ports
- IEEE 802.1x with voice VLAN to permit an IP phone access to the voice VLAN regardless of the authorized or unauthorized state of the port
- IEEE 802.1x with guest VLAN to provide limited services to non-802.1x-compliant users
- IEEE 802.1x accounting to track network usage.
- Network Edge Access Topology (NEAT) with 802.1X switch supplicant, host authorization with CISP, and auto enablement to authenticate a switch outside a wiring closet as a supplicant to another switch.
- TACACS+, a proprietary feature for managing network security through a TACACS server
- RADIUS for verifying the identity of, granting access to, and tracking the actions of remote users through authentication, authorization, and accounting (AAA) services
- Kerberos security system to authenticate requests for network resources by using a trusted third party (requires the cryptographic [that is, supports encryption] version of the switch software image)
- Password recovery disable capability to protect access to switches at customer sites
- DHCP snooping to filter untrusted DHCP messages between untrusted hosts and DHCP servers
- IP source guard to restrict traffic on nonrouted interfaces by filtering traffic based on the DHCP snooping database and IP source bindings
- Dynamic ARP inspection to prevent malicious attacks on the switch by not relaying invalid ARP requests and responses to other ports in the same VLAN
- Secure Socket Layer Version 3.0 support for the HTTP 1.1 server authentication, encryption, and message integrity, and HTTP client authentication to allow secure HTTP communications (requires a cryptographic version of the switch image)
- IEEE 802.1x readiness check to determine the readiness of connected end hosts before configuring IEEE 802.1x on the switch
- Support for IP source guard on static hosts.
- IEEE 802.1x User Distribution to allow deployments with multiple VLANs (for a group of users) to improve scalability of the network by load balancing users across different VLANs. Authorized users are assigned to the least populated VLAN in the group, assigned by RADIUS server.
- Support for 3DES and AES with version 3 of the Simple Network Management Protocol (SNMPv3). This release adds support for the 168-bit Triple Data Encryption Standard (3DES) and the 128-bit, 192-bit, and 256-bit Advanced Encryption Standard (AES) encryption algorithms to SNMPv3.
- Additional IPv6 support to include IPv6 eBGP, IPv6 SNMP, Syslog, and HTTP as well as IPv6 MLD snooping.

QoS Features

- Standard QoS to classify, police, mark, queue, and schedule incoming traffic on a standard port or on an ES port, as well as queue and schedule outgoing traffic on a standard port
  Classification
  - IP type-of-service/Differentiated Services Code Point (IP ToS/DSCP) and 802.1p CoS marking priorities on a per-port basis for protecting the performance of mission-critical applications
- IP ToS/DSCP and 802.1p CoS marking based on flow-based packet classification (classification based on information in the MAC, IP, and TCP/UDP headers) for high-performance quality of service at the network edge, allowing for differentiated service levels for different types of network traffic and for prioritizing mission-critical traffic in the network
- Trusted port states (CoS, DSCP, and IP precedence) within a QoS domain and with a port bordering another QoS domain
- Trusted boundary for detecting the presence of a Cisco IP phone, trusting the CoS value received, and ensuring port security
- DSCP transparency to prevent the switch from rewriting the DSCP field in the user IP packet when QoS is enabled

Policing and out-of-profile marking
- Traffic-policing policies on the switch port for managing how much of the port bandwidth should be allocated to a specific traffic flow (single-rate traffic policing)
- Aggregate policing for policing traffic flows in aggregate to restrict specific applications or traffic flows to metered, predefined rates
- Out-of-profile markdown for packets that exceed bandwidth utilization limits (drop policy actions are passing through the packet without modification, marking down the assigned DSCP in the packet, or dropping the packet)

Ingress queueing and scheduling
- Two configurable ingress queues for user traffic (one queue can be the priority queue)
- Weighted tail drop (WTD) as the congestion-avoidance mechanism for managing the queue lengths and providing drop precedences for different traffic classifications
- Shaped round robin (SRR) as the scheduling service for determining the rate at which packets are dequeued to the internal ring (sharing is the only supported mode on ingress queues)

Egress queues and scheduling
- Four egress queues per port
- An egress priority queue on a standard port. Shaped round robin (SRR) services the priority queue until it is empty before servicing the other three queues
- WTD as the congestion-avoidance mechanism for managing the queue lengths and providing drop precedences for different traffic classifications
- SRR as the scheduling service for determining the rate at which packets are dequeued to the egress interface (shaping or sharing is supported on egress queues). Shaped egress queues are guaranteed but limited to using a share of port bandwidth. Shared egress queues are also guaranteed a configured share of bandwidth, but can use more than the guarantee if other queues become empty and do not use their share of the bandwidth.
- Configurable control-plane queue assignment to assign control plane traffic for CPU-generated traffic to a specific egress queue

• Hierarchical QoS on ES ports or EtherChannels containing ES ports to classify, police, mark, queue, and schedule incoming or outgoing traffic

Classification
- Three QoS configuration levels in the hierarchy: class, VLAN, and physical interface
- Classification based on the CoS value, the DSCP value, the IP precedence value, the MPLS experimental (EXP) bits, or the VLAN

Policing and out-of-profile marking
- Two-rate traffic policing based on the committed information rate (CIR) and the peak information rate (PIR)
- Out-of-profile markdown for packets that exceed bandwidth utilization limits (policy actions are to send packets that conform without modification, to mark down the priority of packets that exceed, and to drop packets that violate)

Egress queueing and scheduling
- Each packet assigned to an egress queue based on the traffic class and VLAN
- Weighted Random Early Detection (WRED) as the congestion-avoidance mechanism
- Class-based weighted fair queuing (CBWFQ) as a queue scheduling management feature to provide guaranteed bandwidth to particular traffic classes, such as voice, that are delay sensitive, while still fairly serving all other traffic in the network
- Low-latency queuing (LLQ) as a scheduling congestion-management feature to provide strict-priority queuing for a traffic class and to enable delay-sensitive data, such as voice, to be sent before packets in other queues are sent
- Traffic shaping to decrease the burstiness of Internet traffic

- Automatic QoS (auto-QoS) to simplify the deployment of existing QoS features by classifying traffic and configuring egress queues
- Support for IPv6 QoS trust capability.

Layer 3 Features

- HSRP Version 1 (HSRPv1) and HSRP Version 2 (HSRPv2) for Layer 3 router redundancy
- IP routing protocols for load balancing and for constructing scalable, routed backbones:
  - RIP Versions 1 and 2
  - OSPF
  - Enhanced Interior Gateway Routing Protocol GRP (EIGRP)
  - Border Gateway Protocol (BGP) Version 4
  - Bidirectional Forwarding Detection (BFD) Protocol to detect forwarding-path failures for OSPF, IS-IS, BGP, EIGRP, or HSRP routing protocols
  - Support for the BFD Protocol on SVIs
- IP routing between VLANs (inter-VLAN routing) for full Layer 3 routing between two or more VLANs, allowing each VLAN to maintain its own autonomous data-link domain
- Policy-based routing (PBR) for configuring defined policies for traffic flows
- Multiple VPN routing/forwarding (multi-VRF) instances in customer edge (CE) devices to allow service providers to support multiple virtual private networks (VPNs) and overlap IP addresses between VPNS (requires the EMI)
- Fallback bridging for forwarding non-IP traffic between two or more VLANs
- Static IP routing for manually building a routing table of network path information
- Equal-cost routing for load balancing and redundancy
- Internet Control Message Protocol (ICMP) and ICMP Router Discovery Protocol (IRDP) for using router advertisement and router solicitation messages to discover the addresses of routers on directly attached subnets
- Protocol-Independent Multicast (PIM) for multicast routing within the network, allowing for devices in the network to receive the multicast feed requested and for switches not participating in the multicast to be pruned. Includes support for PIM sparse mode (PIM-SM), PIM dense mode (PIM-DM), and PIM sparse-dense mode.
- Multicast Source Discovery Protocol (MSDP) for connecting multiple PIM-SM domains
- Distance Vector Multicast Routing Protocol (DVMRP) tunnelling for interconnecting two multicast-enabled networks across non-multicast networks
- DHCP relay for forwarding UDP broadcasts, including IP address requests, from DHCP clients
- Support for IPv6 unicast routing, neighbor discovery, default router preference, DHCP server and relay, IPv6 eBGP, IPv6 SNMP, Syslog, and HTTP as well as IPv6 MLD snooping. Also supports IPv6 QoS trust functionality.

### Monitoring Features

- Switch LEDs that provide port- and switch-level status
- MAC address notification traps and RADIUS accounting for tracking users on a network by storing the MAC addresses that the switch has learned or removed
- Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) for traffic monitoring on any standard port or VLAN.

**Note**
An ES port cannot be a SPAN source.

- SPAN and RSPAN support of Intrusion Detection Systems (IDS) to monitor, repel, and report network security violations
- Four groups (history, statistics, alarms, and events) of embedded RMON agents for network monitoring and traffic analysis
- Syslog facility for logging system messages about authentication or authorization errors, resource issues, and time-out events
- Layer 2 traceroute to identify the physical path that a packet takes from a source device to a destination device
- SFP module diagnostic management interface to monitor physical or operational status of an SFP module.
- Enhanced object tracking for HSRP or IP SLAs clients
- EOT and IP SLAs EOT static route support to identify when a preconfigured static route or a DHCP route goes down
- Support for EEM 3.2, which introduces event detectors for Neighbor Discovery, Identity, and MAC-Address-Table.
- Support for the TWAMP standard for measuring round-trip network performance between any two devices that support the protocol.
The switch is designed for plug-and-play operation, requiring only that you assign basic IP information to the switch and connect it to the other devices in your network. If you have specific network needs, you can change the interface-specific and system-wide settings.

If you do not configure the switch at all, the switch operates with the default settings listed in Table 1-1. This table lists the key software features, their defaults, and where to find more information about the features.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
<th>More information in...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch IP address, subnet mask, and default gateway</td>
<td>0.0.0.0</td>
<td>Chapter 3, “Assigning the Switch IP Address and Default Gateway”</td>
</tr>
<tr>
<td>Domain name</td>
<td>None</td>
<td>Chapter 5, “Administering the Switch”</td>
</tr>
<tr>
<td>Passwords</td>
<td>None defined</td>
<td></td>
</tr>
<tr>
<td>TACACS+</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>RADIUS</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>System name and prompt</td>
<td>Switch</td>
<td></td>
</tr>
<tr>
<td>NTP</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>DNS</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>IEEE 802.1x</td>
<td>Disabled</td>
<td>Chapter 8, “Configuring IEEE 802.1x Port-Based Authentication”</td>
</tr>
<tr>
<td>DHCP client</td>
<td>Enabled (only if the device acting as a DHCP server is configured and is enabled)</td>
<td>Chapter 3, “Assigning the Switch IP Address and Default Gateway”</td>
</tr>
<tr>
<td>DHCP server</td>
<td>Enabled (only if the device is acting as a DHCP relay agent is configured and is enabled)</td>
<td>Chapter 21, “Configuring DHCP Features and IP Source Guard”</td>
</tr>
<tr>
<td>Port parameters</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating mode</td>
<td>Layer 2 (switchport)</td>
<td>Chapter 9, “Configuring Interface Characteristics”</td>
</tr>
<tr>
<td>Port enable state</td>
<td>All ports are enabled.</td>
<td></td>
</tr>
<tr>
<td>Interface speed and duplex mode</td>
<td>Autonegotiate</td>
<td></td>
</tr>
<tr>
<td>Auto MDIX</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>Flow control</td>
<td>Off</td>
<td></td>
</tr>
<tr>
<td>VLANs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Default VLAN</td>
<td>VLAN 1</td>
<td>Chapter 11, “Configuring VLANs”</td>
</tr>
<tr>
<td>VLAN trunking</td>
<td>Dynamic auto (DTP)</td>
<td></td>
</tr>
<tr>
<td>Trunk encapsulation</td>
<td>Negotiate</td>
<td></td>
</tr>
<tr>
<td>VTP mode</td>
<td>Server</td>
<td>Chapter 12, “Configuring VTP”</td>
</tr>
<tr>
<td>VTP version</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Voice VLAN</td>
<td>Disabled</td>
<td>Chapter 14, “Configuring Voice VLAN”</td>
</tr>
</tbody>
</table>
### Table 1-1 Default Settings After Initial Switch Configuration (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
<th>More information in...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private VLANs</td>
<td>None configured.</td>
<td>Chapter 13, “Configuring Private VLANs”</td>
</tr>
<tr>
<td>Dynamic ARP inspection</td>
<td>Disabled on all VLANs</td>
<td>Chapter 22, “Configuring Dynamic ARP Inspection”</td>
</tr>
<tr>
<td><strong>Tunneling</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>802.1Q tunneling</td>
<td>Disabled</td>
<td>Chapter 15, “Configuring IEEE 802.1Q and Layer 2 Protocol Tunneling”</td>
</tr>
<tr>
<td>VLAN mapping</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>Layer 2 protocol tunneling</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td><strong>Spanning Tree Protocol</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>STP</td>
<td>PVST+ enabled on VLAN 1</td>
<td>Chapter 16, “Configuring STP”</td>
</tr>
<tr>
<td>MSTP</td>
<td>Disabled</td>
<td>Chapter 17, “Configuring MSTP”</td>
</tr>
<tr>
<td>Optional spanning-tree features</td>
<td>Disabled</td>
<td>Chapter 18, “Configuring Optional Spanning-Tree Features”</td>
</tr>
<tr>
<td><strong>Flex Links</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Not configured</td>
<td>Chapter 20, “Configuring Flex Links and the MAC Address-Table Move Update Feature”</td>
</tr>
<tr>
<td><strong>DHCP snooping</strong></td>
<td>Disabled</td>
<td>Chapter 21, “Configuring DHCP Features and IP Source Guard”</td>
</tr>
<tr>
<td><strong>IP source guard</strong></td>
<td>Disabled</td>
<td>Chapter 21, “Configuring DHCP Features and IP Source Guard”</td>
</tr>
<tr>
<td>IGMP snooping</td>
<td>Enabled</td>
<td>Chapter 23, “Configuring IGMP Snooping and MVR”</td>
</tr>
<tr>
<td>IGMP filters</td>
<td>None applied</td>
<td></td>
</tr>
<tr>
<td>MVR</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>IGMP throttling</td>
<td>Deny</td>
<td>Chapter 23, “Configuring IGMP Snooping and MVR”</td>
</tr>
<tr>
<td><strong>Port-based Traffic</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Broadcast, multicast, and unicast storm control</td>
<td>Disabled</td>
<td>Chapter 24, “Configuring Port-Based Traffic Control”</td>
</tr>
<tr>
<td>Protected ports</td>
<td>None defined</td>
<td></td>
</tr>
<tr>
<td>Udpcast and multicast traffic flooding</td>
<td>Not blocked</td>
<td></td>
</tr>
<tr>
<td>Secure ports</td>
<td>None configured</td>
<td></td>
</tr>
<tr>
<td>CDP</td>
<td>Enabled</td>
<td>Chapter 25, “Configuring CDP”</td>
</tr>
<tr>
<td>UDLD</td>
<td>Disabled</td>
<td>Chapter 27, “Configuring UDLD”</td>
</tr>
<tr>
<td>SPAN and RSPAN</td>
<td>Disabled</td>
<td>Chapter 28, “Configuring SPAN and RSPAN”</td>
</tr>
<tr>
<td>RMON</td>
<td>Disabled</td>
<td>Chapter 29, “Configuring RMON”</td>
</tr>
<tr>
<td>Syslog messages</td>
<td>Enabled; displayed on the console</td>
<td>Chapter 30, “Configuring System Message Logging”</td>
</tr>
</tbody>
</table>
This section provides network configuration concepts and includes examples of using the switch to create dedicated network segments and interconnecting the segments through Fast Ethernet and Gigabit Ethernet connections.

- “Multidwelling or Ethernet-to-the Subscriber Network” section on page 1-15
- “Layer 2 VPN Application” section on page 1-16
- “Layer 3 VPN Application” section on page 1-17

Table 1-1  Default Settings After Initial Switch Configuration (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
<th>More information in...</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP</td>
<td>Enabled; Version 1</td>
<td>Chapter 31, “Configuring SNMP”</td>
</tr>
<tr>
<td>ACLs</td>
<td>None configured</td>
<td>Chapter 33, “Configuring Network Security with ACLs”</td>
</tr>
<tr>
<td>QoS</td>
<td>Disabled</td>
<td>Chapter 34, “Configuring QoS”</td>
</tr>
<tr>
<td>EtherChannels</td>
<td>None configured</td>
<td>Chapter 35, “Configuring EtherChannels and Link-State Tracking”</td>
</tr>
<tr>
<td>IP unicast routing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP routing (and routing protocols)</td>
<td>Disabled</td>
<td>Chapter 36, “Configuring IP Unicast Routing”</td>
</tr>
<tr>
<td>Multi-VRF-CE</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>MPLS services</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Label switching</td>
<td>Globally enabled; disabled per interface</td>
<td>Chapter 44, “Configuring MPLS, MPLS VPN, MPLS OAM, and EoMPLS”</td>
</tr>
<tr>
<td>EoMPLS</td>
<td>Not configured</td>
<td></td>
</tr>
<tr>
<td>MPLS QoS</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>H-VPLS</td>
<td>No VFiS configured</td>
<td></td>
</tr>
<tr>
<td>Cisco IOS IP SLAs</td>
<td>No operations configured</td>
<td>Chapter 41, “Configuring Cisco IOS IP SLAs Operations”</td>
</tr>
<tr>
<td>HSRP groups</td>
<td>None configured</td>
<td>Chapter 40, “Configuring HSRP”</td>
</tr>
<tr>
<td>IP multicast routing</td>
<td>Disabled on all interfaces</td>
<td>Chapter 45, “Configuring IP Multicast Routing”</td>
</tr>
<tr>
<td>MSDP</td>
<td>Disabled</td>
<td>Chapter 46, “Configuring MSDP”</td>
</tr>
<tr>
<td>Fallback bridging</td>
<td>Not configured</td>
<td>Chapter 47, “Configuring Fallback Bridging”</td>
</tr>
<tr>
<td>Ethernet OAM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CFM(IEEE 802.1ag)</td>
<td>Disabled globally, enabled per interface</td>
<td>Chapter 43, “Configuring Ethernet OAM, CFM, and E-LMI”</td>
</tr>
<tr>
<td>E-LMI</td>
<td>Disabled globally</td>
<td></td>
</tr>
<tr>
<td>Ethernet OAM protocol (IEEE 802.3ah)</td>
<td>Disabled on all interfaces</td>
<td></td>
</tr>
<tr>
<td>Enhanced object tracking</td>
<td>No tracked objects or list configured</td>
<td>Chapter 40, “Configuring HSRP”</td>
</tr>
</tbody>
</table>
Multidwelling or Ethernet-to-the Subscriber Network

Figure 1-1 shows a Gigabit Ethernet ring for a residential location serving multitenant units using Catalyst 3750 Metro switches connected through 1000BASE-X SFP module ports. Catalyst 3750 Metro switches used as residential switches provide customers with high-speed connections to the service provider point-of-presence (POP). Catalyst 2950 Long-Reach Ethernet (LRE) switches also can be used as residential switches for customers requiring connectivity through existing phone lines. The Catalyst 2950 LRE switches can then connect to another residential switch, such as a Catalyst 3750 Metro switch. For more information about the Catalyst LRE switches and LRE information, see the Catalyst 2950 LRE documentation set.

All ports on the residential switches (and Catalyst 2950 LRE switches if they are included) are configured as 802.1Q trunks with Private VLAN Edge (protected port) and STP root guard features enabled. The protected-port feature provides security and isolation between ports on the switch, ensuring that subscribers cannot view packets destined for other subscribers. STP root guard prevents unauthorized devices from becoming the STP root switch. All ports have IGMP snooping or CGMP enabled for multicast traffic management. ACLs on the uplink ports to the aggregating switches provide security and bandwidth management.

The aggregating switches and routers have HSRP enabled for load balancing and redundant connectivity to guarantee mission-critical traffic. This ensures connectivity to the Internet, WAN, and mission-critical network resources in case one of the routers or switches fails.

When an end station in one VLAN needs to communicate with an end station in another VLAN, a router or switch routes the traffic to the appropriate destination VLAN, providing inter-VLAN routing. VLAN access control lists (VLAN maps) provide intra-VLAN security and prevent unauthorized users from accessing critical pieces of the network.

In addition to inter-VLAN routing, the switch QoS mechanisms such as DSCP prioritize the different types of network traffic to deliver high-priority traffic in a predictable manner. If congestion occurs, QoS drops low-priority traffic to allow delivery of high-priority traffic.

The routers also provide firewall services, Network Address Translation (NAT) services, voice-over-IP (VoIP) gateway services, and WAN and Internet access.
Layer 2 VPN Application

You can use Catalyst 3750 Metro switches to form Layer 2 VPNs so that customers at different locations can exchange information through a service-provider network, without requiring dedicated connections. IEEE 802.1Q and Layer 2 protocol tunneling are features designed for service providers who carry traffic of multiple customers across their networks and are required to maintain the VLAN and Layer 2 protocol configurations of each customer without impacting the traffic of other customers.

The Catalyst 3750 Metro switches are used as the provider edge customer-located equipment (PE-CLE) in customer sites at the both edges of the provider network connected to customer premises equipment (CPE) switches. The PE switches tag packets entering the service-provider network with the customer VLAN ID. VLAN mapping translates each customer VLAN ID to a service-provider VLAN ID for transport across the service-provider network. At the egress PE interface, the egress PE switch restores the original VLAN ID numbers for the customer’s network.

The service provider can use 802.1Q tunneling or EoMPLS to provide Layer 2 VPN services. If the service-provider network is an MPLS cloud, and EoMPLS is configured as the point-to-point protocol, MPLS tags are added at the PE-CLE ES port that connects to the MPLS network. The MPLS tags are removed at the ES port of the remote PE-CLE device.

See Chapter 15, “Configuring IEEE 802.1Q and Layer 2 Protocol Tunneling,” and Chapter 44, “Configuring MPLS, MPLS VPN, MPLS OAM, and EoMPLS,” for more information on configuring these features.
Layer 3 VPN Application

Layer 3 VPN services can use multi-VRF-CE or MPLS VPNs to deploy and administer scalable Layer 3 VPN services to business customers. A Layer 3 VPN is a secure IP-based network that shares resources on one or more physical networks. It contains geographically dispersed sites that can communicate securely over a shared backbone.

Figure 1-3 shows an end-to-end MPLS VPN network with MPLS extending from customer site to customer site. The CE devices (which can be Catalyst 3750 Metro switches or other Layer 3 switches) use a routing protocol, such as RIP, EBGP, OSPF, IS-IS, or static routing, to forward packets from customer VPNs to the Catalyst 3750 Metro PE-CLE devices at the edge of the MPLS network. The PE-CLE device is configured with multiprotocol BGP (MP-BGP) and a route distinguisher that is associated with the customer’s VPN. The PE-CLE device converts this information to a VPN-IPv4 format and adds layer distribution protocol (LDP) labels to establish VPN routes.

VPN routes are distributed over the MPLS network using MP-BGP, which also distributes the labels associated with each VPN route. MPLS VPN depends on VPN routing and forwarding (VRF) support to isolate the routing domains from each other.

When an MPLS-VPN packet is received on a port, the CE switch looks up the labels in the routing table to determine what to do with the packet. A PE-CLE router binds a label to each customer prefix learned from a CE device and includes the label in the prefix that it advertises to other PE-CLE routers. When a
PE-CLE router forwards a packet across the provider network, it labels the packet with the label learned from the destination router. When the destination router receives the labeled packet, it examines the label and uses it to direct the packet to the correct CE device.

Only the PE-CLE routers at each end of the MPLS network maintain the VPN routes for VPN members. Provider routers in the core network do not maintain the VPN routes. This ensures the security of customer VPNs and isolates them from other customer packets that are carried across the service-provider MPLS network.

Figure 1-3  MPLS VPN Configuration

See Chapter 44, “Configuring MPLS, MPLS VPN, MPLS OAM, and EoMPLS,” for more information on configuring MPLS VPN.

Where to Go Next

Before configuring the switch, review these sections for startup information:

- Chapter 2, “Using the Command-Line Interface”
- Chapter 3, “Assigning the Switch IP Address and Default Gateway”
- Chapter 4, “Configuring Cisco IOS Configuration Engine”
Using the Command-Line Interface

This chapter describes the Cisco IOS command-line interface (CLI) and how to use it to configure your Catalyst 3750 Metro switch. It contains these sections:

- Understanding Command Modes, page 2-1
- Understanding the Help System, page 2-3
- Understanding Abbreviated Commands, page 2-3
- Understanding no and default Forms of Commands, page 2-4
- Understanding CLI Error Messages, page 2-4
- Using Command History, page 2-4
- Using Editing Features, page 2-6
- Searching and Filtering Output of show and more Commands, page 2-8
- Accessing the CLI, page 2-9

Understanding Command Modes

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

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

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

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

Table 2-1 describes the main command modes, how to access each one, the prompt you see in that mode, and how to exit the mode. The examples in the table use the host name `Switch`. 
### Table 2-1 Command Mode Summary

<table>
<thead>
<tr>
<th>Mode</th>
<th>Access Method</th>
<th>Prompt</th>
<th>Exit Method</th>
<th>About This Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>User EXEC</td>
<td>Begin a session with your switch.</td>
<td><code>Switch&gt;</code></td>
<td>Enter <code>logout</code> or <code>quit</code>.</td>
<td>Use this mode to</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Change terminal settings.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Perform basic tests.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Display system information.</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td>While in user EXEC mode, enter the <code>enable</code> command.</td>
<td><code>Switch#</code></td>
<td>Enter <code>disable</code> to exit.</td>
<td>Use this mode to verify commands that you have entered. Use a password to</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>protect access to this mode.</td>
</tr>
<tr>
<td>Global configuration</td>
<td>While in privileged EXEC mode, enter the <code>configure</code> command.</td>
<td><code>Switch(config)#</code></td>
<td>To exit to privileged EXEC mode, enter <code>exit</code> or <code>end</code>, or press <code>Ctrl-Z</code>.</td>
<td>Use this mode to configure parameters that apply to the entire switch.</td>
</tr>
<tr>
<td>VLAN configuration</td>
<td>While in global configuration mode, enter the <code>vlan vlan-id</code> command.</td>
<td><code>Switch(config-vlan)#</code></td>
<td>To exit to global configuration mode, enter the <code>exit</code> command. To return to privileged EXEC mode, press <code>Ctrl-Z</code> or enter <code>end</code>.</td>
<td>Use this mode to configure VLAN parameters. When VTP mode is transparent, you can create extended-range VLANs (VLAN IDs greater than 1005) and save configurations in the switch startup configuration file.</td>
</tr>
<tr>
<td>Interface configuration</td>
<td>While in global configuration mode, enter the <code>interface</code> command (with a specific interface).</td>
<td><code>Switch(config-if)#</code></td>
<td>To exit to global configuration mode, enter <code>exit</code>. To return to privileged EXEC mode, press <code>Ctrl-Z</code> or enter <code>end</code>.</td>
<td>Use this mode to configure parameters for the Ethernet ports. For information about defining interfaces, see the “Using Interface Configuration Mode” section on page 9-7. To configure multiple interfaces with the same parameters, see the “Configuring a Range of Interfaces” section on page 9-8.</td>
</tr>
<tr>
<td>Line configuration</td>
<td>While in global configuration mode, specify a line with the <code>line vty</code> or <code>line console</code> command.</td>
<td><code>Switch(config-line)#</code></td>
<td>To exit to global configuration mode, enter <code>exit</code>. To return to privileged EXEC mode, press <code>Ctrl-Z</code> or enter <code>end</code>.</td>
<td>Use this mode to configure parameters for the terminal line.</td>
</tr>
</tbody>
</table>
For more detailed information on the command modes, see the command reference for this release.

**Understanding the Help System**

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

**Table 2-2 Help Summary**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>help</td>
<td>Obtain a brief description of the help system in any command mode.</td>
</tr>
<tr>
<td>abbreviated-command-entry?</td>
<td>Obtain a list of commands that begin with a particular character string. For example:</td>
</tr>
<tr>
<td></td>
<td>Switch# di? dir disable disconnect</td>
</tr>
<tr>
<td>abbreviated-command-entry&lt;Tab&gt;</td>
<td>Complete a partial command name. For example:</td>
</tr>
<tr>
<td></td>
<td>Switch# sh conf&lt;tab&gt; Switch# show configuration</td>
</tr>
<tr>
<td>?</td>
<td>List all commands available for a particular command mode. For example:</td>
</tr>
<tr>
<td></td>
<td>Switch&gt; ?</td>
</tr>
<tr>
<td>command ?</td>
<td>List the associated keywords for a command. For example:</td>
</tr>
<tr>
<td></td>
<td>Switch&gt; show ?</td>
</tr>
<tr>
<td>command keyword ?</td>
<td>List the associated arguments for a keyword. For example:</td>
</tr>
<tr>
<td></td>
<td>Switch(config)# cdp holdtime ? &lt;10-255&gt; Length of time (in sec) that receiver must keep this packet</td>
</tr>
</tbody>
</table>

**Understanding Abbreviated Commands**

You need to enter only enough characters for the switch to recognize the command as unique.

This example shows how to enter the `show configuration` privileged EXEC command in an abbreviated form:

`Switch# show conf`
Understanding no and default Forms of Commands

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

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

Understanding CLI Error Messages

Table 2-3 lists some error messages that you might encounter while using the CLI to configure your switch.

**Table 2-3  Common CLI Error Messages**

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

Using Command History

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

- Changing the Command History Buffer Size, page 2-5 (optional)
- Recalling Commands, page 2-5 (optional)
- Disabling the Command History Feature, page 2-5 (optional)
Changing the Command History Buffer Size

By default, the switch records ten command lines in its history buffer. You can alter this number for a current terminal session or for all sessions on a particular line. These procedures are optional.

Beginning in privileged EXEC mode, enter this command to change the number of command lines that the switch records during the current terminal session:

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

The range is from 0 to 256.

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

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

The range is from 0 to 256.

Recalling Commands

To recall commands from the history buffer, perform one of the actions listed in Table 2-4. These actions are optional.

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

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

Disabling the Command History Feature

The command history feature is automatically enabled. You can disable it for the current terminal session or for the command line. These procedures are optional.

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

To disable command history for the line, enter the no history line configuration command.
Using Editing Features

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

- Enabling and Disabling Editing Features, page 2-6 (optional)
- Editing Commands through Keystrokes, page 2-6 (optional)
- Editing Command Lines that Wrap, page 2-8 (optional)

Enabling and Disabling Editing Features

Although enhanced editing mode is automatically enabled, you can disable it, re-enable it, or configure a specific line to have enhanced editing. These procedures are optional.

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

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

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

```
Switch# terminal editing
```

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

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

Editing Commands through Keystrokes

Table 2-5 shows the keystrokes that you need to edit command lines. These keystrokes are optional.

<table>
<thead>
<tr>
<th>Capability</th>
<th>Keystroke1</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Move around the command line to make changes or corrections.</td>
<td>Press Ctrl-B, or press the left arrow key.</td>
<td>Move the cursor back one character.</td>
</tr>
<tr>
<td></td>
<td>Press Ctrl-F, or press the right arrow key.</td>
<td>Move the cursor forward one character.</td>
</tr>
<tr>
<td></td>
<td>Press Ctrl-A.</td>
<td>Move the cursor to the beginning of the command line.</td>
</tr>
<tr>
<td></td>
<td>Press Ctrl-E.</td>
<td>Move the cursor to the end of the command line.</td>
</tr>
<tr>
<td></td>
<td>Press Esc B.</td>
<td>Move the cursor back one word.</td>
</tr>
<tr>
<td></td>
<td>Press Esc F.</td>
<td>Move the cursor forward one word.</td>
</tr>
<tr>
<td></td>
<td>Press Ctrl-T.</td>
<td>Transpose the character to the left of the cursor with the character located at the cursor.</td>
</tr>
<tr>
<td>Recall commands from the buffer and paste them in the command line. The switch provides a buffer with the last ten items that you deleted.</td>
<td>Press Ctrl-Y.</td>
<td>Recall the most recent entry in the buffer.</td>
</tr>
</tbody>
</table>
### Using Editing Features

Press **Esc Y**. Recall the next buffer entry.

The buffer contains only the last 10 items that you have deleted or cut. If you press **Esc Y** more than ten times, you cycle to the first buffer entry.

Delete entries if you make a mistake or change your mind.

Press the **Delete** or **Backspace** key. Erase the character to the left of the cursor.

Press **Ctrl-D**. Delete the character at the cursor.

Press **Ctrl-K**. Delete all characters from the cursor to the end of the command line.

Press **Ctrl-U** or **Ctrl-X**. Delete all characters from the cursor to the beginning of the command line.

Press **Ctrl-W**. Delete the word to the left of the cursor.

Press **Esc D**. Delete from the cursor to the end of the word.

Capitalize or lowercase words or capitalize a set of letters.

Press **Esc C**. Capitalize at the cursor.

Press **Esc L**. Change the word at the cursor to lowercase.

Press **Esc U**. Capitalize letters from the cursor to the end of the word.

Designate a particular keystroke as an executable command, perhaps as a shortcut.

Press **Ctrl-V** or **Esc Q**.

Scroll down a line or screen on displays that are longer than the terminal screen can display.

Press the **Return** key. Scroll down one line.

Press the **Space** bar. Scroll down one screen.

Redisplay the current command line if the switch suddenly sends a message to your screen.

Press **Ctrl-L** or **Ctrl-R**. Redisplay the current command line.

---

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

---

### Table 2-5 Editing Commands through Keystrokes (continued)

<table>
<thead>
<tr>
<th>Capability</th>
<th>Keystroke</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete entries if you make a mistake or change your mind.</td>
<td>Press the <strong>Delete</strong> or <strong>Backspace</strong> key.</td>
<td>Erase the character to the left of the cursor.</td>
</tr>
<tr>
<td>Delete entries if you make a mistake or change your mind.</td>
<td>Press <strong>Esc C</strong>.</td>
<td>Capitalize at the cursor.</td>
</tr>
<tr>
<td>Capitalize or lowercase words or capitalize a set of letters.</td>
<td>Press <strong>Esc L</strong>.</td>
<td>Change the word at the cursor to lowercase.</td>
</tr>
<tr>
<td>Designate a particular keystroke as an executable command, perhaps as a shortcut.</td>
<td>Press <strong>Ctrl-V</strong> or <strong>Esc Q</strong>.</td>
<td></td>
</tr>
<tr>
<td>Scroll down a line or screen on displays that are longer than the terminal screen can display.</td>
<td>Press the <strong>Return</strong> key.</td>
<td>Scroll down one line.</td>
</tr>
<tr>
<td>Redisplay the current command line if the switch suddenly sends a message to your screen.</td>
<td>Press <strong>Ctrl-L</strong> or <strong>Ctrl-R</strong>.</td>
<td>Redisplay the current command line.</td>
</tr>
</tbody>
</table>
Editing Command Lines that Wrap

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

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

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

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

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

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

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

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

Use line wrapping with the command history feature to recall and modify previous complex command entries. For information about recalling previous command entries, see the “Editing Commands through Keystrokes” section on page 2-6.

Searching and Filtering Output of show and more Commands

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

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

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

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

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

```
Switch# show interfaces | include protocol
Vlan1 is up, line protocol is up
Vlan10 is up, line protocol is down
GigabitEthernet1/0/1 is up, line protocol is down
GigabitEthernet1/0/2 is up, line protocol is up
```
Accessing the CLI

You can access the CLI through a console connection or through Telnet. Before you can access the CLI, you must connect a terminal or PC to the switch console port and power on the switch as described in the hardware installation guide that shipped with your switch. Then, to understand the boot process and the options available for assigning IP information, see Chapter 3, “Assigning the Switch IP Address and Default Gateway.”

If your switch is already configured, you can access the CLI through a local console connection or through a remote Telnet session, but your switch must first be configured for this type of access. For more information, see the “Setting a Telnet Password for a Terminal Line” section on page 7-6.

You can use one of these methods to establish a connection with the switch:

- Connect the switch console port to a management station or dial-up modem. For information about connecting to the console port, see the switch hardware installation guide.
- Use any Telnet TCP/IP or encrypted Secure Shell (SSH) package from a remote management station. The switch must have network connectivity with the Telnet or SSH client, and the switch must have an enable secret password configured.

For information about configuring the switch for Telnet access, see the “Setting a Telnet Password for a Terminal Line” section on page 7-6. The switch supports up to 16 simultaneous Telnet sessions. Changes made by one Telnet user are reflected in all other Telnet sessions.

For information about configuring the switch for SSH, see the “Configuring the Switch for Secure Shell” section on page 7-36. The switch supports up to five simultaneous secure SSH sessions.

After you connect through the console port, through a Telnet session, or through an SSH session, the user EXEC prompt appears on the management station.
Assigning the Switch IP Address and Default Gateway

This chapter describes how to create the initial switch configuration (for example, assigning the switch IP address and default gateway information) for the Catalyst 3750 Metro switch by using a variety of automatic and manual methods. It also describes how to modify the switch startup configuration.

For complete syntax and usage information for the commands used in this chapter, see the command reference for this release and to the Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2.

This chapter consists of these sections:
- Understanding the Boot Process, page 3-1
- Assigning Switch Information, page 3-2
- Checking and Saving the Running Configuration, page 3-15
- Modifying the Startup Configuration, page 3-15
- Scheduling a Reload of the Software Image, page 3-19

Understanding the Boot Process

To start your switch, you need to follow the procedures in the hardware installation guide about installing and powering on the switch, and setting up the initial configuration (IP address, subnet mask, default gateway, secret and Telnet passwords, and so forth) of the switch.

The normal boot process involves the operation of the boot loader software, which performs these activities:

- Performs low-level CPU initialization. It initializes the CPU registers, which control where physical memory is mapped, its quantity, its speed, and so forth.
- Performs power-on self-test (POST) for the CPU subsystem. It tests the CPU DRAM and the portion of the flash device that makes up the flash file system.
- Initializes the flash file system on the system board.
- Loads a default operating system software image into memory and boots the switch.
The boot loader provides access to the flash file system before the operating system is loaded. Normally, the boot loader is used only to load, uncompress, and launch the operating system. After the boot loader gives the operating system control of the CPU, the boot loader is not active until the next system reset or power-on.

The boot loader also provides trap-door access into the system if the operating system has problems serious enough that it cannot be used. The trap-door mechanism provides enough access to the system so that if it is necessary, you can format the flash file system, reinstall the operating system software image by using the XMODEM Protocol, recover from a lost or forgotten password, and finally restart the operating system. For more information, see the “Recovering from Corrupted Software By Using the XMODEM Protocol” section on page 48-2 and the “Recovering from a Lost or Forgotten Password” section on page 48-3.

You can disable password recovery. For more information, see the “Disabling Password Recovery” section on page 7-5.

Before you can assign switch information, make sure you have connected a PC or terminal to the console port, and configured the PC or terminal-emulation software baud rate and character format to match these of the switch console port:

- Baud rate default is 9600.
- Data bits default is 8.
- Stop bits default is 1.
- Parity settings default is none.

### Assigning Switch Information

You can assign IP information through the switch setup program, through a DHCP server, or manually. Use the switch setup program if you want to be prompted for specific IP information. With this program, you can also configure a hostname and an enable secret password. It gives you the option of assigning a Telnet password (to provide security during remote management) and configuring your switch as a command or member switch of a cluster or as a standalone switch. For more information about the setup program, see the hardware installation guide.

Use a DHCP server for centralized control and automatic assignment of IP information after the server is configured.

If you are using DHCP, do not respond to any of the questions in the setup program until the switch receives the dynamically-assigned IP address and reads the configuration file.

If you are an experienced user familiar with the switch configuration steps, manually configure the switch. Otherwise, use the setup program described previously.
This section contains this configuration information:

- Default Switch Information, page 3-3
- Understanding DHCP-Based Autoconfiguration, page 3-3
- Manually Assigning IP Information, page 3-14

Default Switch Information

Table 3-1 shows the default switch information.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address and subnet mask</td>
<td>No IP address or subnet mask are defined.</td>
</tr>
<tr>
<td>Default gateway</td>
<td>No default gateway is defined.</td>
</tr>
<tr>
<td>Enable secret password</td>
<td>No password is defined.</td>
</tr>
<tr>
<td>Hostname</td>
<td>The factory-assigned default hostname is Switch.</td>
</tr>
<tr>
<td>Telnet password</td>
<td>No password is defined.</td>
</tr>
<tr>
<td>Cluster command switch function</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Cluster name</td>
<td>No cluster name is defined.</td>
</tr>
</tbody>
</table>

Understanding DHCP-Based Autoconfiguration

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, in which designated DHCP servers allocate network addresses and deliver configuration parameters to dynamically configured devices. The switch can act as both a DHCP client and a DHCP server.

During DHCP-based autoconfiguration, your switch (DHCP client) is automatically configured at startup with IP address information and a configuration file.

With DHCP-based autoconfiguration, no DHCP client-side configuration is needed on your switch. However, you need to configure the DHCP server for various lease options associated with IP addresses. If you are using DHCP to relay the configuration file location on the network, you might also need to configure a Trivial File Transfer Protocol (TFTP) server and a Domain Name System (DNS) server.

The DHCP server for your switch can be on the same LAN or on a different LAN than the switch. If the DHCP server is running on a different LAN, you should configure a DHCP relay device between your switch and the DHCP server. 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 is invoked and requests configuration information from a DHCP server when the configuration file is not present on the switch. If the configuration file is present and the configuration includes the `ip address dhcp` interface configuration command on specific routed interfaces, the DHCP client is invoked and requests the IP address information for those interfaces.

Figure 3-1 shows the sequence of messages that are exchanged between the DHCP client and the DHCP server.

![Figure 3-1 DHCP Client and Server Message Exchange](image)

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 21-10.

If the configuration parameters sent to the client in the DHCPOFFER unicast message 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 that the offered configuration parameters have not been assigned, that an error has occurred during the negotiation of the parameters, or that the client has been slow in responding to the DHCPOFFER message (the DHCP server assigned the parameters to another client).

A DHCP client might receive offers from multiple DHCP or BOOTP servers and can accept any 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 is 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 broadcasts, instead of unicasts, TFTP requests to obtain the switch configuration file.

The DHCP hostname option allows a group of switches to obtain hostnames and a standard configuration from the central management DHCP server. A client (switch) includes in its DCHPDISCover message an option 12 field used to request a hostname and other configuration parameters from the DHCP server. The configuration files on all clients are identical except for their DHCP-obtained hostnames.

If a client has a default hostname (the `hostname name` global configuration command is not configured or the `no hostname` global configuration command is entered to remove the hostname), the DHCP hostname option is not included in the packet when you enter the `ip address dhcp` interface.
configuration command. In this case, if the client receives the DCHP hostname option from the DHCP interaction while acquiring an IP address for an interface, the client accepts the DHCP hostname option and sets the flag to show that the system now has a hostname configured.

**Understanding DHCP-based Autoconfiguration and Image Update**

You can use the DHCP image upgrade features to configure a DHCP server to download both a new image and a new configuration file to one or more switches in a network. This helps ensure that each new switch added to a network receives the same image and configuration.

There are two types of DHCP image upgrades: DHCP autoconfiguration and DHCP auto-image update.

**DHCP Autoconfiguration**

DHCP autoconfiguration downloads a configuration file to one or more switches in your network from a DHCP server. The downloaded configuration file becomes the running configuration of the switch. It does not overwrite the bootup configuration saved in the flash, until you reload the switch.

**DHCP Auto-Image Update**

You can use DHCP auto-image upgrade with DHCP auto configuration to download both a configuration and a new image to one or more switches in your network. The switch (or switches) downloading the new configuration and the new image can be blank (or only have a default factory configuration loaded).

If the new configuration is downloaded to a switch that already has a configuration, the downloaded configuration is appended to the configuration file stored on the switch. (Any existing configuration is not overwritten by the downloaded one.)

To enable a DHCP auto-image update on the switch, the TFTP server where the image and configuration files are located must be configured with the correct option 67 (the configuration filename), option 66 (the DHCP server hostname) option 150 (the TFTP server address), and option 125 (description of the file) settings.

For procedures to configure the switch as a DHCP server, see the “Configuring DHCP-Based Autoconfiguration” section on page 3-6 and the “Configuring DHCP” section of the “IP addressing and Services” section of the *Cisco IOS IP Configuration Guide, Release 12.2*.

After you install the switch in your network, the auto-image update feature starts. The downloaded configuration file is saved in the running configuration of the switch, and the new image is downloaded and installed on the switch. When you reboot the switch, the configuration is stored in the saved configuration on the switch.

**Limitations and Restrictions**

These are the limitations:

- The DHCP-based autoconfiguration with a saved configuration process stops if there is not at least one Layer 3 interface in an up state without an assigned IP address in the network.
- Unless you configure a timeout, the DHCP-based autoconfiguration with a saved configuration feature tries indefinitely to download an IP address.
Assigning Switch Information

Chapter 3 Assigning the Switch IP Address and Default Gateway

Assigning Switch Information

The auto-install process stops if a configuration file cannot be downloaded or it the configuration file is corrupted.

Note

The configuration file that is downloaded from TFTP is merged with the existing configuration in the running configuration but is not saved in the NVRAM unless you enter the `write memory` or `copy running-configuration startup-configuration` privileged EXEC command. Note that if the downloaded configuration is saved to the startup configuration, the feature is not triggered during subsequent system restarts.

Configuring DHCP-Based Autoconfiguration

These sections describe how to configure DHCP-based autoconfiguration.

- DHCP Server Configuration Guidelines, page 3-6
- Configuring the TFTP Server, page 3-7
- Configuring the DNS, page 3-7
- Configuring the Relay Device, page 3-8
- Obtaining Configuration Files, page 3-8
- Example Configuration, page 3-9

If your DHCP server is a Cisco device, see the “Configuring DHCP” section of the “IP Addressing and Services” section of the *Cisco IOS IP Configuration Guide, Release 12.2* for additional information about configuring DHCP.

DHCP Server Configuration Guidelines

Follow these guidelines if you are configuring a device as a DHCP server:

You should configure the DHCP server with reserved leases that are bound to each switch by the switch hardware address.

If you want the switch to receive IP address information, you must configure the DHCP server with these lease options:

- IP address of the client (required)
- Subnet mask of the client (required)
- DNS server IP address (optional)
- Router IP address (default gateway address to be used by the switch) (required)

If you want the switch to receive the configuration file from a TFTP server, you must configure the DHCP server with these lease options:

- TFTP server name (required)
- Boot filename (the name of the configuration file that the client needs) (recommended)
- Hostname (optional)

Depending on the settings of the DHCP server, the switch can receive IP address information, the configuration file, or both.
If you do not configure the DHCP server with the lease options described previously, it replies to client requests with only those parameters that are configured. If the IP address and the subnet mask are not in the reply, the switch is not configured. If the router IP address or the TFTP server name are not found, the switch might send broadcast, instead of unicast, TFTP requests. Unavailability of other lease options does not affect autoconfiguration.

The switch can act as a DHCP server. By default, the Cisco IOS DHCP server and relay agent features are enabled on your switch but are not configured. These features are not operational. If your DHCP server is a Cisco device, for additional information about configuring DHCP, see the “Configuring DHCP” section of the “IP Addressing and Services” section of the Cisco IOS IP Configuration Guide from the Cisco.com page under Documentation > Cisco IOS Software > 12.2 Mainline > Configuration Guides.

**Configuring the TFTP Server**

Based on the DHCP server configuration, the switch attempts to download one or more configuration files from the TFTP server. If you configured the DHCP server to respond to the switch with all the options required for IP connectivity to the TFTP server, and if you configured the DHCP server with a TFTP server name, address, and configuration filename, the switch attempts to download the specified configuration file from the specified TFTP server.

If you did not specify the configuration filename, the TFTP server, or if the configuration file could not be downloaded, the switch attempts to download a configuration file by using various combinations of filenames and TFTP server addresses. The files include the specified configuration filename (if any) and these files: network-config, cisconet.cfg, hostname.config, or hostname.cfg, where hostname is the switch’s current hostname. The TFTP server addresses used include the specified TFTP server address (if any) and the broadcast address (255.255.255.255).

For the switch to successfully download a configuration file, the TFTP server must contain one or more configuration files in its base directory. The files can include these files:

- The configuration file named in the DHCP reply (the actual switch configuration file).
- The network-config or the cisconet.cfg file (known as the default configuration files).
- The router-config or the ciscortr.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.)

If you specify the TFTP server name in the DHCP server-lease database, you must also configure the TFTP server name-to-IP-address mapping in the DNS-server database.

If the TFTP server to be used is on a different LAN from the switch, or if it is to be accessed by the switch through the broadcast address (which occurs if the DHCP server response does not contain all the required information described previously), a relay must be configured to forward the TFTP packets to the TFTP server. For more information, see the “Configuring the Relay Device” section on page 3-8. The preferred solution is to configure the DHCP server with all the required information.

**Configuring the DNS**

The DHCP server uses the DNS server to resolve the TFTP server name to an 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 can 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 on a different LAN as the switch. If it is on a different LAN, the switch must be able to access it through a router.

**Configuring the Relay Device**

You must configure a relay device, also referred to as a relay agent, when a switch sends broadcast packets that require a response from a host on a different LAN. Examples of broadcast packets that the switch might send are DHCP, DNS, and in some cases, TFTP packets. You must configure this relay device to forward received broadcast packets on an interface to the destination host.

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

For example, in Figure 3-2, configure the router interfaces as follows:

On interface 10.0.0.2:

```bash
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

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

**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 these 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, TFTP server address, and the configuration filename from the DHCP server. 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.
The IP address and the configuration filename is reserved for the switch, but the TFTP server address is not provided in the DHCP reply (one-file read method).

The switch receives its IP address, subnet mask, and the configuration filename from the DHCP server. The switch sends a broadcast message to a 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 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, subnet mask, and the TFTP server address from the DHCP server. 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 hostnames-to-IP-address mapping for the switch. The switch fills its host table with the information in the file and obtains its hostname. If the hostname is not found in the file, the switch uses the hostname in the DHCP reply. If the hostname is not specified in the DHCP reply, the switch uses the default Switch as its hostname.

After obtaining its hostname from the default configuration file or the DHCP reply, the switch reads the configuration file that has the same name as its hostname (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 hostname file, it reads the router-config file. If the switch cannot read the router-config file, it reads the ciscortr.cfg file.

Note

The switch broadcasts TFTP server requests if the TFTP server 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 3-3 shows a sample network for retrieving IP information by using DHCP-based autoconfiguration.

Table 3-2 shows the configuration of the reserved leases on the DHCP server.
**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 hostname to be assigned to the switch based on its IP address. The base directory also contains a configuration file for each switch (*switcha-confg*, *switchb-confg*, and so forth) as shown in this display:

```
prompt> cd /tftpserver/work/
prompt> ls
network-confg
switcha-confg
switchb-confg
switchc-confg
switchd-confg
prompt> cat network-confg
ip host switcha 10.0.0.21
ip host switchb 10.0.0.22
ip host switchc 10.0.0.23
ip host switchd 10.0.0.24
```

**DHCP Client Configuration**

No configuration file is present on Switch A through Switch D.

**Configuration Explanation**

In Figure 3-3, Switch A 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 A reads the network-confg file from the base directory of the TFTP server.
- It adds the contents of the network-confg file to its host table.
- It reads its host table by indexing its IP address 10.0.0.21 to its hostname (switcha).
It reads the configuration file that corresponds to its hostname; for example, it reads switcha-config from the TFTP server.

Switches B through D retrieve their configuration files and IP addresses in the same way.

Configuring the DHCP Auto Configuration and Image Update Features

Using DHCP to download a new image and a new configuration to a switch requires that you configure at least two switches: One switch acts as a DHCP and TFTP server. The client switch is configured to download either a new configuration file or a new configuration file and a new image file.

Configuring DHCP Autoconfiguration (Only Configuration File)

Beginning in privileged EXEC mode, follow these steps to configure DHCP autoconfiguration of the TFTP and DHCP settings on a new switch to download a new configuration file.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><strong>configure terminal</strong> Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><strong>ip dhcp poolname</strong> Create a name for the DHCP Server address pool, and enter DHCP pool configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td><strong>bootfile filename</strong> Specify the name of the configuration file that is used as a boot image.</td>
</tr>
<tr>
<td>Step 4</td>
<td><strong>network network-number mask prefix-length</strong> Specify the subnet network number and mask of the DHCP address pool.</td>
</tr>
<tr>
<td>Step 5</td>
<td><strong>default-router address</strong> Specify the IP address of the default router for a DHCP client.</td>
</tr>
<tr>
<td>Step 6</td>
<td><strong>option 150 address</strong> Specify the IP address of the TFTP server.</td>
</tr>
<tr>
<td>Step 7</td>
<td><strong>exit</strong> Return to global configuration mode.</td>
</tr>
<tr>
<td>Step 8</td>
<td><strong>tftp-server flash:filename.text</strong> Specify the configuration file on the TFTP server.</td>
</tr>
<tr>
<td>Step 9</td>
<td><strong>interface interface-id</strong> Specify the address of the client that will receive the configuration file.</td>
</tr>
<tr>
<td>Step 10</td>
<td><strong>no switchport</strong> Put the interface into Layer 3 mode.</td>
</tr>
<tr>
<td>Step 11</td>
<td><strong>ip address address mask</strong> Specify the IP address and mask for the interface.</td>
</tr>
<tr>
<td>Step 12</td>
<td><strong>end</strong> Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 13</td>
<td><strong>copy running-config startup-config</strong> (Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
This example shows how to configure a switch as a DHCP server so that it will download a configuration file:

```plaintext
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(dhcp-config)# network 10.10.10.0 255.255.255.0
Switch(dhcp-config)# bootfile config-boot.text
Switch(dhcp-config)# default-router 10.10.10.1
Switch(dhcp-config)# option 150 10.10.10.1
Switch(dhcp-config)# exit
Switch(config)# tftp-server flash:config-boot.text
Switch(config)# interface gigabitethernet1/0/4
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.10.10.1 255.255.255.0
Switch(config-if)# end
```

### Configuring DHCP Auto-Image Update (Configuration File and Image)

Beginning in privileged EXEC mode, follow these steps to configure DHCP autoconfiguration to configure TFTP and DHCP settings on a new switch to download a new image and a new configuration file.

**Note** Before following the steps in this table, you must create a text file (for example, autoinstall_dhcp) that will be uploaded to the switch. In the text file, put the name of the image that you want to download (for example, c3750m-ipservices-mz.122-44.3.SE.tar). This image must be a tar and not a bin file.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>ip dhcp pool name</td>
<td>Create a name for the DHCP server address pool and enter DHCP pool configuration mode.</td>
</tr>
<tr>
<td>bootfile filename</td>
<td>Specify the name of the file that is used as a boot image.</td>
</tr>
<tr>
<td>network network-number mask prefix-length</td>
<td>Specify the subnet network number and mask of the DHCP address pool.</td>
</tr>
<tr>
<td>default-router address</td>
<td>Specify the IP address of the default router for a DHCP client.</td>
</tr>
<tr>
<td>option 150 address</td>
<td>Specify the IP address of the TFTP server.</td>
</tr>
<tr>
<td>option 125 hex</td>
<td>Specify the path to the text file that describes the path to the image file.</td>
</tr>
<tr>
<td>copy tftp flash filename.txt</td>
<td>Upload the text file to the switch.</td>
</tr>
<tr>
<td>copy tftp flash imagename.tar</td>
<td>Upload the tarfile for the new image to the switch.</td>
</tr>
<tr>
<td>exit</td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td>tftp-server flash:config.text</td>
<td>Specify the Cisco IOS configuration file on the TFTP server.</td>
</tr>
<tr>
<td>tftp-server flash:imagename.tar</td>
<td>Specify the image name on the TFTP server.</td>
</tr>
<tr>
<td>tftp-server flash:filename.txt</td>
<td>Specify the text file that contains the name of the image file to download</td>
</tr>
<tr>
<td>interface interface-id</td>
<td>Specify the address of the client that will receive the configuration file.</td>
</tr>
</tbody>
</table>
### Assigning Switch Information

This example shows how to configure a switch as a DHCP server so it downloads a configuration file:

```plaintext
Switch# config terminal
Switch(config)# ip dhcp pool pool1
Switch(config)# network 10.10.10.0 255.255.255.0
Switch(config)# bootfile config-boot.text
Switch(config)# default-router 10.10.10.1
Switch(config)# option 150 10.10.10.1
Switch(config)# option 125 hex 0000.0009.0a05.0866.1.7574.6f69.7341.6c6c.5f6863
Switch(config)# exit
Switch(config)# tftp-server flash:config-boot.text
Switch(config)# tftp-server flash:c3750m-ipservices-mz.122-44.3.SE.tar
Switch(config)# tftp-server flash:boot-config.text
Switch(config)# tftp-server flash: autoinstall_dhcp
Switch(config)# interface gigabitEthernet1/0/4
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.10.10.1 255.255.255.0
Switch(config-if)# end
```

### Configuring the Client

Beginning in privileged EXEC mode, follow these steps to configure a switch to download a configuration file and new image from a DHCP server:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>boot host dhcp</td>
</tr>
<tr>
<td>Step 3</td>
<td>boot host retry timeout timeout-value</td>
</tr>
<tr>
<td></td>
<td>Note: If you do not set a timeout the system will indefinitely try to obtain an IP address from the DHCP server.</td>
</tr>
<tr>
<td>Step 4</td>
<td>banner config-save ^C warning-message ^C</td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
</tr>
<tr>
<td>Step 6</td>
<td>show boot</td>
</tr>
</tbody>
</table>

This example uses a Layer 3 SVI interface on VLAN 99 to enable DHCP-based autoconfiguration with a saved configuration:

```plaintext
Switch# configure terminal
Switch(config)# boot host dhcp
Switch(config)# boot host retry timeout 300
```
Manually Assigning IP Information

Beginning in privileged EXEC mode, follow these steps to manually assign IP information to multiple switched virtual interfaces (SVIs) or ports:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td>Step 2</td>
<td><strong>interface vlan</strong> <strong>vlan-id</strong></td>
</tr>
<tr>
<td></td>
<td>information is assigned. The range is 1 to 4094; do not enter leading</td>
</tr>
<tr>
<td></td>
<td>zeros.</td>
</tr>
<tr>
<td>Step 3</td>
<td><strong>ip address</strong> <strong>ip-address</strong> <strong>subnet-mask</strong></td>
</tr>
<tr>
<td>Step 4</td>
<td><strong>exit</strong></td>
</tr>
<tr>
<td>Step 5</td>
<td><strong>ip default-gateway</strong> <strong>ip-address</strong></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td><strong>end</strong></td>
</tr>
<tr>
<td>Step 7</td>
<td><strong>show running-config</strong></td>
</tr>
<tr>
<td>Step 8</td>
<td><strong>copy running-config startup-config</strong></td>
</tr>
</tbody>
</table>
Checking and Saving the Running Configuration

You can check the configuration settings you entered or changes you made by entering the `show running-config` privileged EXEC command: For information about the output of this command, see the Cisco IOS Configuration Fundamental Command Reference, Release 12.2.

To store the configuration or changes you have made to your startup configuration in flash memory, enter the `copy running-config startup-config` privileged EXEC command. This command saves the configuration settings that you made. If you fail to do this, your configuration will be lost the next time you reload the system. To display information stored in the NVRAM section of flash memory, use the `show startup-config` or `more startup-config` privileged EXEC command.

For more information about alternative locations to copy the configuration file, see Appendix B, “Working with the Cisco IOS File System, Configuration Files, and Software Images.”

Modifying the Startup Configuration

This section describes how to modify the switch startup configuration. It contains this configuration information:

- Default Boot Configuration, page 3-15
- Automatically Downloading a Configuration File, page 3-16
- Booting Manually, page 3-17
- Booting a Specific Software Image, page 3-17
- Controlling Environment Variables, page 3-18

Default Boot Configuration

Table 3-3 shows the default boot configuration.

To remove the switch IP address, use the `no ip address` interface configuration command. If you are removing the address through a Telnet session, your connection to the switch will be lost. To remove the default gateway address, use the `no ip default-gateway` global configuration command.

For information on setting the switch system name, protecting access to privileged EXEC commands, and setting time and calendar services, see Chapter 5, “Administering the Switch.”
Modifying the Startup Configuration

Automatically Downloading a Configuration File

You can automatically download a configuration file to your switch by using the DHCP-based autoconfiguration feature. For more information, see the “Understanding DHCP-Based Autoconfiguration” section on page 3-3.

Specifying the Filename to Read and Write the System Configuration

By default, the IOS software uses the file config.text to read and write a nonvolatile copy of the system configuration. However, you can specify a different filename, which is loaded during the next boot cycle.

Beginning in privileged EXEC mode, follow these steps to specify a different configuration filename:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>boot config-file flash:file-url</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
</tr>
<tr>
<td>Step 4</td>
<td>show boot</td>
</tr>
<tr>
<td>Step 5</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To return to the default setting, use the no boot config-file global configuration command.
Booting Manually

By default, the switch automatically boots; however, you can configure it to manually boot.
Beginning in privileged EXEC mode, follow these steps to configure the switch to manually boot during the next boot cycle:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 boot manual</td>
<td>Enable the switch to manually boot during the next boot cycle.</td>
</tr>
<tr>
<td>Step 3 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4 show boot</td>
<td>Verify your entries.</td>
</tr>
</tbody>
</table>

The `boot manual` global command changes the setting of the MANUAL_BOOT environment variable.
The next time you reboot the system, the switch is in boot loader mode, shown by the `switch:` prompt. To boot the system, use the `boot filesystem:filesystem:file-url` boot loader command.
- For `filesystem:`, use `flash:` for the system board flash device.
- For `file-url`, specify the path (directory) and the name of the bootable image.
Filenames and directory names are case sensitive.

To disable manual booting, use the `no boot manual` global configuration command.

Booting a Specific Software Image

By default, the switch attempts to automatically boot the system using information in the BOOT environment variable. If this variable is not set, the switch attempts to load and execute the first executable image it can by performing a recursive, depth-first search throughout the flash file system. In a depth-first search of a directory, each encountered subdirectory is completely searched before continuing the search in the original directory. However, you can specify a specific image to boot.
Beginning in privileged EXEC mode, follow these steps to configure the switch to boot a specific image during the next boot cycle:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 boot system filesystem:filesystem:file-url</td>
<td>Configure the switch to boot a specific image in flash memory during the next boot cycle.</td>
</tr>
</tbody>
</table>
  - For `filesystem:`, use `flash:` for the system board flash device.
  - For `file-url`, specify the path (directory) and the name of the bootable image.
Filenames and directory names are case sensitive.
Chapter 3  Assigning the Switch IP Address and Default Gateway  

Modifying the Startup Configuration

To return to the default setting, use the `no boot system` global configuration command.

Controlling Environment Variables

With a normally operating switch, you enter the boot loader mode only through a switch console connection configured for 9600 bps. Unplug the switch power cord and press the switch `Mode` button while reconnecting the power cord. You can release the `Mode` button a second or two after the LED above port 1 turns off. Then the boot loader `switch:` prompt is displayed.

The switch boot loader software provides support for nonvolatile environment variables, which can be used to control how the boot loader, or any other software running on the system, behaves. Boot loader environment variables are similar to environment variables that can be set on UNIX or DOS systems.

Environment variables that have values are stored in flash memory outside of the flash file system. Each line in these files contains an environment variable name and an equal sign followed by the value of the variable. A variable has no value if it is not listed in this file; it has a value if it is listed in the file even if the value is a null string. A variable that is set to a null string (for example, “ ”) is a variable with a value. Many environment variables are predefined and have default values.

Environment variables store two kinds of data:

- Data that controls code, which does not read the IOS configuration file. For example, the name of a boot loader helper file, which extends or patches the functionality of the boot loader can be stored as an environment variable.
- Data that controls code, which is responsible for reading the IOS configuration file. For example, the name of the IOS configuration file can be stored as an environment variable.

You can change the settings of the environment variables by accessing the boot loader or by using IOS commands. Under normal circumstances, it is not necessary to alter the setting of the environment variables.

**Note**  
For complete syntax and usage information for the boot loader commands and environment variables, see the command reference for this release.
Table 3-4 describes the function of the most common environment variables.

### Table 3-4 Environment Variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Boot Loader Command</th>
<th>IOS Global Configuration Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>BOOT</td>
<td>set BOOT filesystem:file-url ...</td>
<td>boot system filesystem:file-url</td>
</tr>
<tr>
<td></td>
<td>A semicolon-separated list of executable files to try to load and execute when automatically booting. If the BOOT environment variable is not set, the system attempts to load and execute the first executable image it can find by using a recursive, depth-first search through the flash file system. If the BOOT variable is set but the specified images cannot be loaded, the system attempts to boot the first bootable file that it can find in the flash file system.</td>
<td>Specifies the IOS image to load during the next boot cycle. This command changes the setting of the BOOT environment variable.</td>
</tr>
<tr>
<td>MANUAL_BOOT</td>
<td>set MANUAL_BOOT yes</td>
<td>boot manual</td>
</tr>
<tr>
<td></td>
<td>Determines whether the switch automatically or manually boots.</td>
<td>Enables manually booting the switch during the next boot cycle and changes the setting of the MANUAL_BOOT environment variable. The next time you reboot the system, the switch is in boot loader mode. To boot the system, use the boot loader boot flash:filesystem:file-url command, and specify the name of the bootable image.</td>
</tr>
<tr>
<td>CONFIG_FILE</td>
<td>set CONFIG_FILE flash:file-url</td>
<td>boot config-file flash:file-url</td>
</tr>
<tr>
<td></td>
<td>Changes the filename that IOS uses to read and write a nonvolatile copy of the system configuration.</td>
<td>Specifies the filename that IOS uses to read and write a nonvolatile copy of the system configuration. This command changes the CONFIG_FILE environment variable.</td>
</tr>
</tbody>
</table>

### Scheduling a Reload of the Software Image

You can schedule a reload of the software image to occur on the switch at a later time (for example, late at night or during the weekend when the switch is used less), or you can synchronize a reload network-wide (for example, to perform a software upgrade on all switches in the network).

**Note**

A scheduled reload must take place within approximately 24 days.

### Configuring a Scheduled Reload

To configure your switch to reload the software image at a later time, use one of these commands in privileged EXEC mode:

- `reload in [hh:]mm [text]`
This command schedules a reload of the software to take affect in the specified minutes or hours and minutes. The reload must take place within approximately 24 days. You can specify the reason for the reload in a string up to 255 characters in length.

- **reload at hh:mm [month day | day month] [text]**

  This command schedules a reload of the software to take place at the specified time (using a 24-hour clock). If you specify the month and day, the reload is scheduled to take place at the specified time and date. If you do not specify the month and day, the reload takes place at the specified time on the current day (if the specified time is later than the current time) or on the next day (if the specified time is earlier than the current time). Specifying 00:00 schedules the reload for midnight.

  **Note**  
  Use the **at** keyword only if the switch system clock has been set (through Network Time Protocol (NTP), the hardware calendar, or manually). The time is relative to the configured time zone on the switch. To schedule reloads across several switches to occur simultaneously, the time on each switch must be synchronized with NTP.

  The **reload** command halts the system. If the system is not set to manually boot, it reboots itself. Use the **reload** command after you save the switch configuration information to the startup configuration (**copy running-config startup-config**).

  If your switch is configured for manual booting, do not reload it from a virtual terminal. This restriction prevents the switch from entering the boot loader mode and thereby taking it from the remote user’s control.

  If you modify your configuration file, the switch prompts you to save the configuration before reloading. During the save operation, the system requests whether you want to proceed with the save if the CONFIG_FILE environment variable points to a startup configuration file that no longer exists. If you proceed in this situation, the system enters setup mode upon reload.

  This example shows how to reload the software on the switch on the current day at 7:30 p.m:

  ```
  Switch# reload at 19:30
  Reload scheduled for 19:30:00 UTC Wed Jun 5 2003 (in 2 hours and 25 minutes)
  Proceed with reload? [confirm]
  ```

  This example shows how to reload the software on the switch at a future time:

  ```
  Switch# reload at 02:00 jun 20
  Reload scheduled for 02:00:00 UTC Thu Jun 20 2003 (in 344 hours and 53 minutes)
  Proceed with reload? [confirm]
  ```

  To cancel a previously scheduled reload, use the **reload cancel** privileged EXEC command.

### Displaying Scheduled Reload Information

To display information about a previously scheduled reload or to determine if a reload has been scheduled on the switch, use the **show reload** privileged EXEC command.

It displays reload information including the time the reload is scheduled to occur and the reason for the reload (if it was specified when the reload was scheduled).
Configuring Cisco IOS Configuration Engine

This chapter describes how to configure the feature on the Catalyst 3750 Metro switch.

Note


This chapter consists of these sections:

- Understanding Cisco Configuration Engine Software, page 4-1
- Understanding Cisco IOS Agents, page 4-5
- Configuring Cisco IOS Agents, page 4-6
- Displaying CNS Configuration, page 4-15

Understanding Cisco Configuration Engine Software

The Cisco Configuration Engine is network management software that acts as a configuration service for automating the deployment and management of network devices and services (see Figure 4-1). Each Configuration Engine manages a group of Cisco devices (switches and routers) and the services that they deliver, storing their configurations and delivering them as needed. The Configuration Engine automates initial configurations and configuration updates by generating device-specific configuration changes, sending them to the device, executing the configuration change, and logging the results.

The Configuration Engine supports standalone and server modes and has these CNS components:

- Configuration service (web server, file manager, and namespace mapping server)
- Event service (event gateway)
- Data service directory (data models and schema)

In standalone mode, the Configuration Engine supports an embedded Directory Service. In this mode, no external directory or other data store is required. In server mode, the Configuration Engine supports the use of a user-defined external directory.
These sections contain this conceptual information:

- Configuration Service, page 4-2
- Event Service, page 4-3
- What You Should Know About the CNS IDs and Device Hostnames, page 4-3

**Configuration Service**

The Configuration Service is the core component of the Cisco Configuration Engine. It consists of a configuration server that works with Cisco IOS CNS agents on the switch. The Configuration Service delivers device and service configurations to the switch for initial configuration and mass reconfiguration by logical groups. Switches receive their initial configuration from the Configuration Service when they start up on the network for the first time.

The Configuration Service uses the CNS Event Service to send and receive configuration change events and to send success and failure notifications.

The configuration server is a web server that uses configuration templates and the device-specific configuration information stored in the embedded (standalone mode) or remote (server mode) directory. Configuration templates are text files containing static configuration information in the form of CLI commands. In the templates, variables are specified using Lightweight Directory Access Protocol (LDAP) URLs that reference the device-specific configuration information stored in a directory.

The Cisco IOS agent can perform a syntax check on received configuration files and publish events to show the success or failure of the syntax check. The configuration agent can either apply configurations immediately or delay the application until receipt of a synchronization event from the configuration server.
Event Service

The Cisco Configuration Engine uses the Event Service for receipt and generation of configuration events. The event agent is on the switch and facilitates the communication between the switch and the event gateway on the Configuration Engine.

The Event Service is a highly capable publish-and-subscribe communication method. The Event Service uses subject-based addressing to send messages to their destinations. Subject-based addressing conventions define a simple, uniform namespace for messages and their destinations.

NameSpace Mapper

The Configuration Engine includes the NameSpace Mapper (NSM) that provides a lookup service for managing logical groups of devices based on application, device or group ID, and event.

Cisco IOS devices recognize only event subject-names that match those configured in Cisco IOS software; for example, cisco.cns.config.load. You can use the namespace mapping service to designate events by using any desired naming convention. When you have populated your data store with your subject names, NSM changes your event subject-name strings to those known by Cisco IOS.

For a subscriber, when given a unique device ID and event, the namespace mapping service returns a set of events to which to subscribe. Similarly, for a publisher, when given a unique group ID, device ID, and event, the mapping service returns a set of events on which to publish.

What You Should Know About the CNS IDs and Device Hostnames

The Configuration Engine assumes that a unique identifier is associated with each configured switch. This unique identifier can take on multiple synonyms, where each synonym is unique within a particular namespace. The event service uses namespace content for subject-based addressing of messages.

The Configuration Engine intersects two namespaces, one for the event bus and the other for the configuration server. Within the scope of the configuration server namespace, the term ConfigID is the unique identifier for a device. Within the scope of the event bus namespace, the term DeviceID is the CNS unique identifier for a device.

Because the Configuration Engine uses both the event bus and the configuration server to provide configurations to devices, you must define both ConfigID and Device ID for each configured switch.

Within the scope of a single instance of the configuration server, no two configured switches can share the same value for ConfigID. Within the scope of a single instance of the event bus, no two configured switches can share the same value for DeviceID.

ConfigID

Each configured switch has a unique ConfigID, which serves as the key into the Configuration Engine directory for the corresponding set of switch CLI attributes. The ConfigID defined on the switch must match the ConfigID for the corresponding switch definition on the Configuration Engine.

The ConfigID is fixed at startup time and cannot be changed until the device restarts, even if the switch hostname is reconfigured.
DeviceID

Each configured switch participating on the event bus has a unique DeviceID, which is analogous to the switch source address so that the switch can be targeted as a specific destination on the bus. All switches configured with the `cns config partial` global configuration command must access the event bus. Therefore, the DeviceID, as originated on the switch, must match the DeviceID of the corresponding switch definition in the Configuration Engine.

The origin of the DeviceID is defined by the Cisco IOS hostname of the switch. However, the DeviceID variable and its usage reside within the event gateway adjacent to the switch.

The logical Cisco IOS termination point on the event bus is embedded in the event gateway, which in turn functions as a proxy on behalf of the switch. The event gateway represents the switch and its corresponding DeviceID to the event bus.

The switch declares its hostname to the event gateway immediately after the successful connection to the event gateway. The event gateway couples the DeviceID value to the Cisco IOS hostname each time this connection is established. The event gateway caches this DeviceID value for the duration of its connection to the switch.

Hostname and DeviceID

The DeviceID is fixed at the time of the connection to the event gateway and does not change even when the switch hostname is reconfigured.

When changing the switch hostname on the switch, the only way to refresh the DeviceID is to break the connection between the switch and the event gateway. Enter the `no cns event` global configuration command followed by the `cns event` global configuration command.

When the connection is re-established, the switch sends its modified hostname to the event gateway. The event gateway redefines the DeviceID to the new value.

**Caution**

When using the Configuration Engine user interface, you must first set the DeviceID field to the hostname value that the switch acquires *after*—not *before*—you use the `cns config initial` global configuration command at the switch. Otherwise, subsequent `cns config partial` global configuration command operations malfunction.

Using Hostname, DeviceID, and ConfigID

In standalone mode, when a hostname value is set for a switch, the configuration server uses the hostname as the DeviceID when an event is sent on hostname. If the hostname has not been set, the event is sent on the `cn=<value>` of the device.

In server mode, the hostname is not used. In this mode, the unique DeviceID attribute is always used for sending an event on the bus. If this attribute is not set, you cannot update the switch.

These and other associated attributes (tag value pairs) are set when you run **Setup** on the Configuration Engine.

**Note**

Understanding Cisco IOS Agents

The CNS event agent feature allows the switch to publish and subscribe to events on the event bus and works with the Cisco IOS agent. The Cisco IOS agent feature supports the switch by providing these features:

- Initial Configuration, page 4-5
- Incremental (Partial) Configuration, page 4-6
- Synchronized Configuration, page 4-6

Initial Configuration

When the switch first comes up, it attempts to get an IP address by broadcasting a DHCP request on the network. Assuming there is no DHCP server on the subnet, the distribution switch acts as a DHCP relay agent and forwards the request to the DHCP server. Upon receiving the request, the DHCP server assigns an IP address to the new switch and includes the TFTP server IP address, the path to the bootstrap configuration file, and the default gateway IP address in a unicast reply to the DHCP relay agent. The DHCP relay agent forwards the reply to the switch.

The switch automatically configures the assigned IP address on interface VLAN 1 (the default) and downloads the bootstrap configuration file from the TFTP server. Upon successful download of the bootstrap configuration file, the switch loads the file in its running configuration.

The Cisco IOS agents initiate communication with the Configuration Engine by using the appropriate ConfigID and EventID. The Configuration Engine maps the Config ID to a template and downloads the full configuration file to the switch.

Figure 4-2 shows a sample network configuration for retrieving the initial bootstrap configuration file by using DHCP-based autoconfiguration.
Incremental (Partial) Configuration

After the network is running, new services can be added by using the Cisco IOS agent. Incremental (partial) configurations can be sent to the switch. The actual configuration can be sent as an event payload by way of the event gateway (push operation) or as a signal event that triggers the switch to initiate a pull operation.

The switch can check the syntax of the configuration before applying it. If the syntax is correct, the switch applies the incremental configuration and publishes an event that signals success to the configuration server. If the switch does not apply the incremental configuration, it publishes an event showing an error status. When the switch has applied the incremental configuration, it can write it to NVRAM or wait until signaled to do so.

Synchronized Configuration

When the switch receives a configuration, it can defer application of the configuration upon receipt of a write-signal event. The write-signal event tells the switch not to save the updated configuration into its NVRAM. The switch uses the updated configuration as its running configuration. This ensures that the switch configuration is synchronized with other network activities before saving the configuration in NVRAM for use at the next reboot.

Configuring Cisco IOS Agents

The Cisco IOS agents embedded in the switch Cisco IOS software allow the switch to be connected and automatically configured as described in the “Enabling Automated CNS Configuration” section on page 4-6. If you want to change the configuration or install a custom configuration, see these sections for instructions:

- Enabling the CNS Event Agent, page 4-7
- Enabling the Cisco IOS CNS Agent, page 4-9
- Upgrading Devices with Cisco IOS Image Agent, page 4-14

Enabling Automated CNS Configuration

To enable automated CNS configuration of the switch, you must first complete the prerequisites in Table 4-1. When you complete them, power on the switch. At the setup prompt, do nothing: The switch begins the initial configuration as described in the “Initial Configuration” section on page 4-5. When the full configuration file is loaded on your switch, you need to do nothing else.

<table>
<thead>
<tr>
<th>Device</th>
<th>Required Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access switch</td>
<td>Factory default (no configuration file)</td>
</tr>
<tr>
<td>Distribution switch</td>
<td>• IP helper address</td>
</tr>
<tr>
<td></td>
<td>• Enable DHCP relay agent</td>
</tr>
<tr>
<td></td>
<td>• IP routing (if used as default gateway)</td>
</tr>
</tbody>
</table>
Table 4-1  Prerequisites for Enabling Automatic Configuration (continued)

<table>
<thead>
<tr>
<th>Device</th>
<th>Required Configuration</th>
</tr>
</thead>
</table>
| DHCP server             | • IP address assignment  
                            | • TFTP server IP address  
                            | • Path to bootstrap configuration file on the TFTP server  
                            | • Default gateway IP address                                              |
| TFTP server             | • A bootstrap configuration file that includes the CNS configuration commands that enable the switch to communicate with the Configuration Engine  
                            | • The switch configured to use either the switch MAC address or the serial number (instead of the default hostname) to generate the ConfigID and EventID  
                            | • The CNS event agent configured to push the configuration file to the switch |
| CNS Configuration Engine | One or more templates for each type of device, with the ConfigID of the device mapped to the template. |

Note: For more information about running the setup program and creating templates on the Configuration Engine, see the Cisco Configuration Engine Installation and Setup Guide, 1.5 for Linux at http://www.cisco.com/en/US/docs/net_mgmt/configuration_engine/1.5/installation_linux/guide/setup_1.html

**Enabling the CNS Event Agent**

Note: You must enable the CNS event agent on the switch before you enable the CNS configuration agent.
Beginning in privileged EXEC mode, follow these steps to enable the CNS event agent on the switch:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enable the event agent, and enter the gateway parameters.</td>
</tr>
<tr>
<td>cns event {hostname</td>
<td>ip-address} [port-number] [backup] [failover-time seconds] [keepalive seconds] [retry-count] [source ip-address]</td>
</tr>
<tr>
<td></td>
<td>• (Optional) For port number, enter the port number for the event gateway. The default port number is 11011.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) Enter backup to show that this is the backup gateway. (If omitted, this is the primary gateway.)</td>
</tr>
<tr>
<td></td>
<td>• (Optional) For failover-time seconds, enter how long the switch waits for the primary gateway route after the route to the backup gateway is established.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) For keepalive seconds, enter how often the switch sends keepalive messages. For retry-count, enter the number of unanswered keepalive messages that the switch sends before the connection is terminated. The default for each is 0.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) For reconnect time, enter the maximum time interval that the switch waits before trying to reconnect to the event gateway.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) For source ip-address, enter the source IP address of this device.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Though visible in the command-line help string, the encrypt and the clock-timeout time keywords are not supported.</td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>show cns event connections</td>
<td>Verify information about the event agent.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
</tbody>
</table>

To disable the CNS event agent, use the `no cns event {ip-address | hostname}` global configuration command.

This example shows how to enable the CNS event agent, set the IP address gateway to 10.180.1.27, set 120 seconds as the keepalive interval, and set 10 as the retry count.

```
Switch(config)# cns event 10.180.1.27 keepalive 120 10
```
### Enabling the Cisco IOS CNS Agent

After enabling the CNS event agent, start the Cisco IOS CNS agent on the switch. You can enable the Cisco IOS agent with these commands:

- The `cns config initial` global configuration command enables the Cisco IOS agent and initiates an initial configuration on the switch.
- The `cns config partial` global configuration command enables the Cisco IOS agent and initiates a partial configuration on the switch. You can then use the Configuration Engine to remotely send incremental configurations to the switch.

### Enabling an Initial Configuration

Beginning in privileged EXEC mode, follow these steps to enable the CNS configuration agent and initiate an initial configuration on the switch:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>cns template connect name</code></td>
<td>Enter CNS template connect configuration mode, and specify the name of the CNS connect template.</td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>cli config-text</code></td>
<td>Enter a command line for the CNS connect template. Repeat this step for each command line in the template.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Repeat Steps 2 to 3 to configure another CNS connect template.</td>
</tr>
<tr>
<td><strong>Step 5</strong> <code>exit</code></td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 6</strong> <code>cns connect name [retries number] [retry-interval seconds] [sleep seconds] [timeout seconds]</code></td>
<td>Enter CNS connect configuration mode, specify the name of the CNS connect profile, and define the profile parameters. The switch uses the CNS connect profile to connect to the Configuration Engine.</td>
</tr>
</tbody>
</table>

- Enter the name of the CNS connect profile.
- (Optional) For `retries number`, enter the number of connection retries. The range is 1 to 30. The default is 3.
- (Optional) For `retry-interval seconds`, enter the interval between successive connection attempts to the Configuration Engine. The range is 1 to 40 seconds. The default is 10 seconds.
- (Optional) For `sleep seconds`, enter the amount of time before which the first connection attempt occurs. The range is 0 to 250 seconds. The default is 0.
- (Optional) For `timeout seconds`, enter the amount of time after which the connection attempts end. The range is 10 to 2000 seconds. The default is 120.
### Command

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 7  | discover (controller controller-type | Specify the interface parameters in the CNS connect profile.  
|         | |  
|         | |   • For controller controller-type, enter the controller type.  
|         | |   • For dlci, enter the active data-link connection identifiers (DLCIs).  
|         | |   (Optional) For subinterface subinterface-number, specify the point-to-point subinterface number that is used to search for active DLCIs.  
|         | |   • For interface [interface-type], enter the type of interface.  
|         | |   • For line line-type, enter the line type.  
|         | [subinterface subinterface-number] |                                                                                           |
|         | |                                                                                           |
|         | | [interface-type] |                                                                                           |
|         | | line line-type} |                                                                                           |
| Step 8  | template name [ ... name]            | Specify the list of CNS connect templates in the CNS connect profile to be applied to the switch configuration. You can specify more than one template. |
| Step 9  | exit                                 | Return to global configuration mode.                                                                                                   |
| Step 10 | hostname name                        | Enter the hostname for the switch.                                                                                                 |
| Step 12 | ip route network-number              | (Optional) Establish a static route to the Configuration Engine whose IP address is network-number.                                  |
### Step 13

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`cns id interface num [dns-reverse</td>
<td>ipaddress</td>
</tr>
</tbody>
</table>

- For `interface num`, enter the type of interface—for example, ethernet, group-async, loopback, or virtual-template. This setting specifies from which interface the IP or MAC address should be retrieved to define the unique ID.

- For `{dns-reverse | ipaddress | mac-address}`, enter `dns-reverse` to retrieve the hostname and assign it as the unique ID, enter `ipaddress` to use the IP address, or enter `mac-address` to use the MAC address as the unique ID.

- (Optional) Enter `event` to set the ID to be the event-id value used to identify the switch.

- (Optional) Enter `image` to set the ID to be the image-id value used to identify the switch.

**Note** If both the `event` and `image` keywords are omitted, the image-id value is used to identify the switch.

- For `{hardware-serial | hostname | string string | udi}`, enter `hardware-serial` to set the switch serial number as the unique ID, enter `hostname` (the default) to select the switch hostname as the unique ID, enter an arbitrary text string for `string string` as the unique ID, or enter `udi` to set the unique device identifier (UDI) as the unique ID.
To disable the CNS Cisco IOS agent, use the `no cns config initial {ip-address | hostname}` global configuration command.

This example shows how to configure an initial configuration on a remote switch when the switch configuration is unknown (the CNS Zero Touch feature).

```plaintext
Switch(config)# cns template connect template-dhcp
Switch(config-tmpl-conn)# cli ip address dhcp
Switch(config-tmpl-conn)# exit
Switch(config)# cns template connect ip-route
Switch(config-tmpl-conn)# cli ip route 0.0.0.0 0.0.0.0 ${next-hop}
Switch(config-tmpl-conn)# exit
Switch(config)# cns connect dhcp
Switch(config-cna-conn)# discover interface gigabitethernet
Switch(config-cna-conn)# template template-dhcp
Switch(config-cna-conn)# template ip-route
Switch(config-cna-conn)# exit
Switch(config)# hostname RemoteSwitch
RemoteSwitch(config)# cns config initial 10.1.1.1 no-persist
```
This example shows how to configure an initial configuration on a remote switch when the switch IP address is known. The Configuration Engine IP address is 172.28.129.22.

Switch(config)# cns template connect template-dhcp
Switch(config-tmpl-conn)# cli ip address dhcp
Switch(config-tmpl-conn)# exit
Switch(config)# cns template connect ip-route
Switch(config-tmpl-conn)# cli ip route 0.0.0.0 0.0.0.0 $(next-hop)
Switch(config-tmpl-conn)# exit
Switch(config)# cns connect dhcp
Switch(config-cns-conn)# discover interface gigabitethernet
Switch(config-cns-conn)# template template-dhcp
Switch(config-cns-conn)# template ip-route
Switch(config-cns-conn)# exit
Switch(config)# hostname RemoteSwitch
RemoteSwitch(config)# ip route 172.28.129.22 255.255.255.255 11.11.11.1
RemoteSwitch(config)# cns id ethernet 0 ipaddress
RemoteSwitch(config)# cns config initial 172.28.129.22 no-persist

Enabling a Partial Configuration

Beginning in privileged EXEC mode, follow these steps to enable the Cisco IOS agent and to initiate a partial configuration on the switch:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>cns config partial [ip-address</td>
</tr>
<tr>
<td></td>
<td>• For [ip-address</td>
</tr>
<tr>
<td></td>
<td>• (Optional) For port-number, enter the port number of the configuration server. The default port number is 80.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) Enter source ip-address to use for the source IP address.</td>
</tr>
<tr>
<td></td>
<td>Note Though visible in the command-line help string, the encrypt keyword is not supported.</td>
</tr>
<tr>
<td>Step 3</td>
<td>end Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show cns config stats or show cns config outstanding Verify information about the configuration agent.</td>
</tr>
<tr>
<td>Step 5</td>
<td>show running-config Verify your entries.</td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config (Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable the Cisco IOS agent, use the no cns config partial [ip-address | hostname] global configuration command. To cancel a partial configuration, use the cns config cancel privileged EXEC command.
Upgrading Devices with Cisco IOS Image Agent

Administrators maintaining large networks of Cisco IOS devices need an automated mechanism to load image files onto large numbers of remote devices. Existing network management applications are useful to determine which images to run and how to manage images received from the Cisco online software center. Other image distribution solutions do not scale to cover thousands of devices and cannot distribute images to devices behind a firewall or using Network Address Translation (NAT). The CNS image agent enables the managed device to initiate a network connection and request an image download allowing devices using NAT, or behind firewalls, to access the image server.

You can use image agent to download one or more devices. The switches must have the image agent running on them.

Prerequisites for the CNS Image Agent

Confirm these prerequisites before upgrading one or more devices with image agent:

- Determine where to store the Cisco IOS images on a file server to make the image available to the other networking devices. If the CNS Event Bus is to be used to store and distribute the images, the CNS event agent must be configured.
- Set up a file server to enable the networking devices to download the new images using the HTTPS protocol.
- Determine how to handle error messages generated by image image agent operations. Error messages can be sent to the CNS Event Bus or an HTTP or HTTPS URL.

Restrictions for the CNS Image Agent

During automated image loading operations you must try to prevent the Cisco IOS device from losing connectivity with the file server that is providing the image. Image reloading is subject to memory issues and connection issues. Boot options must also be configured to allow the Cisco IOS device to boot another image if the first image reload fails.

These other restrictions apply to the image agent running on a the switch:

- You can only download the tar image file. Downloading the bin image file is not supported.
- Only the immediate download option is supported. You cannot schedule a download to occur at a specified date and time.
- The Destination field in the Associate Image with Device window is not supported.

For more details, see your CNS IE2100 documentation and see the “File Management” section of the Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2.

Beginning in privileged EXEC mode, follow these steps to initiate the image agent to check for a new image and upgrade a device:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode</td>
</tr>
<tr>
<td>Step 2 ip host {ip-address} {hostname}</td>
<td>Enter the IP address and the hostname of the event gateway.</td>
</tr>
<tr>
<td>Step 3 cns trusted-server all-agents {hostname}</td>
<td>Specify a trusted server for CNS agent.</td>
</tr>
<tr>
<td>Step 4 no cns aaa enable cns event {ip-address} {port number}</td>
<td>Disable AAA authentication on the event gateway.</td>
</tr>
</tbody>
</table>
This example shows how to upgrade a switch from a server with the address of 172.20.249.20:

```
Switch(config)> configure terminal
Switch(config)# ip host cns-dsbu.cisco.com 172.20.249.20
Switch(config)# cns trusted-server all-agents cns-dsbu.cisco.com
Switch(config)# no cns aaa enable cns event 172.20.249.20 22022
Switch(config)# cns image retry 1
Switch(config)# cns image server http://172.20.249.20:80/cns/HttpMsgDispatcher status
http://172.20.249.20:80/cns/HttpMsgDispatcher
Switch(config)# end
```

You can check the status of the image download by using the `show cns image` status user EXEC command.

### Displaying CNS Configuration

You can use the privileged EXEC commands in Table 4-2 to display CNS configuration information.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show cns config connections</code></td>
<td>Displays the status of the CNS Cisco IOS agent connections.</td>
</tr>
<tr>
<td><code>show cns config outstanding</code></td>
<td>Displays information about incremental (partial) CNS configurations that have started but are not yet completed.</td>
</tr>
<tr>
<td><code>show cns config stats</code></td>
<td>Displays statistics about the Cisco IOS agent.</td>
</tr>
<tr>
<td><code>show cns event connections</code></td>
<td>Displays the status of the CNS event agent connections.</td>
</tr>
<tr>
<td><code>show cns event stats</code></td>
<td>Displays statistics about the CNS event agent.</td>
</tr>
<tr>
<td><code>show cns event subject</code></td>
<td>Displays a list of event agent subjects that are subscribed to by applications.</td>
</tr>
</tbody>
</table>
Administering the Switch

This chapter describes how to perform one-time operations to administer the Catalyst 3750 Metro switch.

This chapter consists of these sections:

- Managing the System Time and Date, page 5-1
- Configuring a System Name and Prompt, page 5-14
- Creating a Banner, page 5-17
- Managing the MAC Address Table, page 5-19
- Managing the ARP Table, page 5-31

Managing the System Time and Date

You can manage the system time and date on your switch using automatic configuration, such as the Network Time Protocol (NTP), or manual configuration methods.

Note

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

This section contains this configuration information:

- Understanding the System Clock, page 5-1
- Understanding Network Time Protocol, page 5-2
- Configuring NTP, page 5-3
- Configuring Time and Date Manually, page 5-11

Understanding the System Clock

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

The system clock can then be set from these sources:

- Network Time Protocol
- Manual configuration
The system clock can provide time to these services:

- User `show` commands
- Logging and debugging messages

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

The system clock keeps track of whether the time is authoritative or not (that is, whether it has been set by a time source considered to be authoritative). If it is not authoritative, the time is available only for display purposes and is not redistributed. For configuration information, see the “Configuring Time and Date Manually” section on page 5-11.

**Understanding Network Time Protocol**

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

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

NTP uses the concept of a *stratum* to describe how many NTP hops away a device is from an authoritative time source. A stratum 1 time server has a radio or atomic clock directly attached, a stratum 2 time server receives its time through NTP from a stratum 1 time server, and so on. A device running NTP automatically chooses as its time source the device with the lowest stratum number with which it communicates through NTP. This strategy effectively builds a self-organizing tree of NTP speakers.

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

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

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

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

Figure 5-1 shows a typical network example using NTP. Switch A is the NTP master, with Switches B, C, and D configured in NTP server mode, in server association with Switch A. Switch E is configured as an NTP peer to the upstream and downstream switches, Switch B and Switch F.
If the network is isolated from the Internet, Cisco’s implementation of NTP allows a device to act as though it is synchronized through NTP, when in fact it has determined the time by using other means. Other devices then synchronize to that device through NTP.

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

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

**Configuring NTP**

The switches do not have a hardware-supported clock, and they cannot function as an NTP master clock to which peers synchronize themselves when an external NTP source is not available. These switches also have no hardware support for a calendar. As a result, the `ntp update-calendar` and the `ntp master` global configuration commands are not available.

This section contains this configuration information:

- Default NTP Configuration, page 5-4
- Configuring NTP Authentication, page 5-4
- Configuring NTP Associations, page 5-5
Default NTP Configuration

Table 5-1 shows the default NTP configuration.

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

NTP is enabled on all interfaces by default. All interfaces receive NTP packets.

Configuring NTP Authentication

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

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 ntp authenticate</td>
<td>Enable the NTP authentication feature, which is disabled by default.</td>
</tr>
<tr>
<td>Step 3 ntp authentication-key number md5 value</td>
<td>Define the authentication keys. By default, none are defined.</td>
</tr>
<tr>
<td></td>
<td>- For number, specify a key number. The range is 1 to 4294967295.</td>
</tr>
<tr>
<td></td>
<td>- md5 specifies that message authentication support is provided by using the message digest algorithm 5 (MD5).</td>
</tr>
<tr>
<td></td>
<td>- For value, enter an arbitrary string of up to eight characters for the key.</td>
</tr>
</tbody>
</table>

The switch does not synchronize to a device unless both have one of these authentication keys, and the key number is specified by the ntp trusted-key key-number command.
Managing the System Time and Date

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

This example shows how to configure the switch to synchronize only to devices providing authentication key 42 in the device’s NTP packets:

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

Configuring NTP Associations

An NTP association can be a peer association (this switch can either synchronize to the other device or allow the other device to synchronize to it), or it can be a server association (meaning that only this switch synchronizes to the other device, and not the other way around).
Beginning in privileged EXEC mode, follow these steps to form an NTP association with another device:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>ntp peer ip-address [version number] [key keyid] [source interface] [prefer]</td>
<td>Configure the switch system clock to synchronize a peer or to be synchronized by a peer (peer association).</td>
</tr>
<tr>
<td>or ntp server ip-address [version number] [key keyid] [source interface] [prefer]</td>
<td>Configure the switch system clock to be synchronized by a time server (server association).</td>
</tr>
</tbody>
</table>

No peer or server associations are defined by default.

- For ip-address in a peer association, specify either the IP address of the peer providing, or being provided, the clock synchronization. For a server association, specify the IP address of the time server providing the clock synchronization.

- (Optional) For number, specify the NTP version number. The range is 1 to 3. By default, Version 3 is selected.

- (Optional) For keyid, enter the authentication key defined with the ntp authentication-key global configuration command.

- (Optional) For interface, specify the interface from which to pick the IP source address. By default, the source IP address is taken from the outgoing interface.

- (Optional) Enter the prefer keyword to make this peer or server the preferred one that provides synchronization. This keyword reduces switching back and forth between peers and servers.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

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

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

This example shows how to configure the switch to synchronize its system clock with the clock of the peer at IP address 172.16.22.44 using NTP Version 2:

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

### Configuring NTP Broadcast Service

The communications between devices running NTP (known as associations) are usually statically configured; each device is given the IP addresses of all devices with which it should form associations. Accurate timekeeping is possible by exchanging NTP messages between each pair of devices with an association. However, in a LAN environment, NTP can be configured to use IP broadcast messages instead. This alternative reduces configuration complexity because each device can simply be configured to send or receive broadcast messages. However, the information flow is one-way only.
The switch can send or receive NTP broadcast packets on an interface-by-interface basis if there is an NTP broadcast server, such as a router, broadcasting time information on the network. The switch can send NTP broadcast packets to a peer so that the peer can synchronize to it. The switch can also receive NTP broadcast packets to synchronize its own clock. This section provides procedures for both sending and receiving NTP broadcast packets.

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

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

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

This example shows how to configure a port to send NTP Version 2 packets:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ntp broadcast version 2
```

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>interface interface-id</td>
<td>Specify the interface to receive NTP broadcast packets, and enter interface configuration mode.</td>
</tr>
<tr>
<td>3</td>
<td>ntp broadcast client</td>
<td>Enable the interface to receive NTP broadcast packets. By default, no interfaces receive NTP broadcast packets.</td>
</tr>
<tr>
<td>4</td>
<td>exit</td>
<td>Return to global configuration mode.</td>
</tr>
</tbody>
</table>
To disable a port from receiving NTP broadcast packets, use the `no ntp broadcast client` interface configuration command. To change the estimated round-trip delay to the default, use the `no ntp broadcastdelay` global configuration command.

This example shows how to configure a port to receive NTP broadcast packets:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ntp broadcast client
```

### Configuring NTP Access Restrictions

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

- Creating an Access Group and Assigning a Basic IP Access List, page 5-8
- Disabling NTP Services on a Specific Interface, page 5-9

#### Creating an Access Group and Assigning a Basic IP Access List

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
</tbody>
</table>
| Step 2: ntp access-group { query-only | serve-only | serve | peer } access-list-number | Create an access group, and apply a basic IP access list. The keywords have these meanings:
  - `query-only` — Allows only NTP control queries.
  - `serve-only` — Allows only time requests.
  - `serve` — Allows time requests and NTP control queries, but does not allow the switch to synchronize to the remote device.
  - `peer` — Allows time requests and NTP control queries and allows the switch to synchronize to the remote device.
  
  For `access-list-number`, enter a standard IP access list number from 1 to 99. |

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 5: ntp broadcastdelay microseconds</td>
<td>(Optional) Change the estimated round-trip delay between the switch and the NTP broadcast server. The default is 3000 microseconds; the range is 1 to 999999.</td>
</tr>
<tr>
<td>Step 6: end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 7: show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 8: copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
Managing the System Time and Date

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

1. **peer**—Allows time requests and NTP control queries and allows the switch to synchronize itself to a device whose address passes the access list criteria.

2. **serve**—Allows time requests and NTP control queries, but does not allow the switch to synchronize itself to a device whose address passes the access list criteria.

3. **serve-only**—Allows only time requests from a device whose address passes the access list criteria.

4. **query-only**—Allows only NTP control queries from a device whose address passes the access list criteria.

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

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

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

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

Disabling NTP Services on a Specific Interface

NTP services are enabled on all interfaces by default.
Beginning in privileged EXEC mode, follow these steps to disable NTP packets from being received on an interface:

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

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

### Configuring the Source IP Address for NTP Packets

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

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

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

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

### Displaying the NTP Configuration

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

- `show ntp associations [detail]`
- `show ntp status`
Managing the System Time and Date

For detailed information about the fields in these displays, see the Cisco IOS Configuration Fundamentals Command Reference, Release 12.2.

Configuring Time and Date Manually

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

This section contains this configuration information:

- Setting the System Clock, page 5-11
- Displaying the Time and Date Configuration, page 5-11
- Configuring the Time Zone, page 5-12
- Configuring Summer Time (Daylight Saving Time), page 5-13

Setting the System Clock

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

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>clock set hh:mm:ss day month year</code></td>
<td>Manually set the system clock using one of these formats.</td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td><code>clock set hh:mm:ss month day year</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• For <code>hh:mm:ss</code>, specify the time in hours (24-hour format), minutes, and seconds. The time specified is relative to the configured time zone.</td>
</tr>
<tr>
<td></td>
<td>• For <code>day</code>, specify the day by date in the month.</td>
</tr>
<tr>
<td></td>
<td>• For <code>month</code>, specify the month by name.</td>
</tr>
<tr>
<td></td>
<td>• For <code>year</code>, specify the year (no abbreviation).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td>show running-config</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>copy running-config startup-config</code></td>
</tr>
</tbody>
</table>

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

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

Displaying the Time and Date Configuration

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

The system clock keeps an authoritative flag that shows whether the time is authoritative (believed to be accurate). If the system clock has been set by a timing source such as NTP, the flag is set. If the time is not authoritative, it is used only for display purposes. Until the clock is authoritative and the authoritative flag is set, the flag prevents peers from synchronizing to the clock when the peers’ time is invalid.
The symbol that precedes the `show clock` display has this meaning:
- *—Time is not authoritative.
- (blank)—Time is authoritative.
- .—Time is authoritative, but NTP is not synchronized.

## Configuring the Time Zone

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>clock timezone zone hours-offset</code></td>
<td>Set the time zone. The switch keeps internal time in universal time</td>
</tr>
<tr>
<td></td>
<td></td>
<td>coordinated (UTC), so this command is used only for display purposes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>and when the time is manually set.</td>
</tr>
<tr>
<td></td>
<td>(<code>minutes-offset</code>)</td>
<td>• For <code>zone</code>, enter the name of the time zone to be displayed when</td>
</tr>
<tr>
<td></td>
<td></td>
<td>standard time is in effect. The default is UTC.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For <code>hours-offset</code>, enter the hours offset from UTC.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) For <code>minutes-offset</code>, enter the minutes offset from UTC.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>show running-config</code></td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

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

To set the time to UTC, use the `no clock timezone` global configuration command.
Configuring Summer Time (Daylight Saving Time)

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>clock summer-time zone recurring [week day month hh:mm week day month hh:mm [offset]]</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
</tr>
<tr>
<td>Step 4</td>
<td>show running-config</td>
</tr>
<tr>
<td>Step 5</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

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

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

```
Switch(config)# clock summer-time PDT recurring 1 Sunday April 2:00 last Sunday October 2:00
```
Beginning in privileged EXEC mode, follow these steps if summer time in your area does not follow a recurring pattern (configure the exact date and time of the next summer time events):

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>clock summer-time zone date [month date year hh:mm month date year hh:mm [offset]] or clock summer-time zone date [date month year hh:mm date month year hh:mm [offset]]</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>show running-config</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

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

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

This example shows how to set summer time to start on October 12, 2003, at 02:00, and end on April 26, 2004, at 02:00:

```
Switch(config)# clock summer-time pdt date 12 October 2003 2:00 26 April 2004 2:00
```

### Configuring a System Name and Prompt

You configure the system name on the switch to identify it. By default, the system name and prompt are Switch.

If you have not configured a system prompt, the first 20 characters of the system name are used as the system prompt. A greater-than symbol [>] is appended. The prompt is updated whenever the system name changes.

**Note**

For complete syntax and usage information for the commands used in this section, see the Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 and the Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2.
This section contains this configuration information:

- Default System Name and Prompt Configuration, page 5-15
- Configuring a System Name, page 5-15
- Understanding DNS, page 5-15

Default System Name and Prompt Configuration

The default switch system name and prompt is *Switch*.

Configuring a System Name

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>hostname name</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
</tr>
<tr>
<td>Step 4</td>
<td>show running-config</td>
</tr>
<tr>
<td>Step 5</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

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

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

Understanding DNS

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

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

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

- Default DNS Configuration, page 5-16
- Setting Up DNS, page 5-16
- Displaying the DNS Configuration, page 5-17

Default DNS Configuration

Table 5-2 shows the default DNS configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS enable state</td>
<td>Enabled.</td>
</tr>
<tr>
<td>DNS default domain name</td>
<td>None configured.</td>
</tr>
<tr>
<td>DNS servers</td>
<td>No name server addresses are configured.</td>
</tr>
</tbody>
</table>

Setting Up DNS

Beginning in privileged EXEC mode, follow these steps to set up your switch to use the DNS:

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

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

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

**Note**

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

This section contains this configuration information:

- Default Banner Configuration, page 5-17
- Configuring a Message-of-the-Day Login Banner, page 5-18
- Configuring a Login Banner, page 5-19

### Default Banner Configuration

The MOTD and login banners are not configured.
Creating a Banner

Configuring a Message-of-the-Day Login Banner

You can create a single or multiline message banner that appears on the screen when someone logs in to the switch.

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

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

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

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

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

This example shows the banner displayed from the previous configuration:

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

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

User Access Verification

Password:
```
Configuring a Login Banner

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

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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>banner login (c) message (c)</td>
<td>Specify the login message. For (c), enter the delimiting character of your choice, for example, a pound sign (#), and press the Return key. The delimiting character signifies the beginning and end of the banner text. Characters after the ending delimiter are discarded. For message, enter a login message up to 255 characters. You cannot use the delimiting character in the message.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show running-config</td>
<td>Verify your entries.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

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

This example shows how to configure a login banner for the switch by using the dollar sign ($) symbol as the beginning and ending delimiter:

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

Managing the MAC Address Table

The MAC address table contains address information that the switch uses to forward traffic between ports. All MAC addresses in the address table are associated with one or more ports. The address table includes these types of addresses:

- Dynamic address: a source MAC address that the switch learns and then ages when it is not in use.
- Static address: a manually entered unicast address that does not age and that is not lost when the switch resets.

The address table lists the destination MAC address, the associated VLAN ID, and port number associated with the address and the type (static or dynamic).

**Note**

For complete syntax and usage information for the commands used in this section, see the command reference for this release.
Building the Address Table

With multiple MAC addresses supported on all ports, you can connect any port on the switch to individual workstations, repeaters, switches, routers, or other network devices. The switch provides dynamic addressing by learning the source address of packets it receives on each port and adding the address and its associated port number to the address table. As stations are added or removed from the network, the switch updates the address table, adding new dynamic addresses and aging out those that are not in use.

The aging interval is globally configured. However, the switch maintains an address table for each VLAN, and STP can accelerate the aging interval on a per-VLAN basis.

The switch sends packets between any combination of ports, based on the destination address of the received packet. Using the MAC address table, the switch forwards the packet only to the port associated with the destination address. If the destination address is on the port that sent the packet, the packet is filtered and not forwarded. The switch always uses the store-and-forward method: complete packets are stored and checked for errors before transmission.

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. Unicast addresses, for example, could forward to port 1 in VLAN 1 and ports 9, 10, and 1 in VLAN 5.

Note

Multiport static addresses are not supported.

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.
When private VLANs are configured, address learning depends on the type of MAC address:

- Dynamic MAC addresses learned in one VLAN of a private VLAN are replicated in the associated VLANs. For example, a MAC address learned in a private-VLAN secondary VLAN is replicated in the primary VLAN.

- Static MAC addresses configured in a primary or secondary VLAN are not replicated in the associated VLANs. When you configure a static MAC address in a private VLAN primary or secondary VLAN, you should also configure the same static MAC address in all associated VLANs.

For more information about private VLANs, see Chapter 13, “Configuring Private VLANs.”

You can disable MAC address learning on a per-VLAN basis. Customers in a service provider network can tunnel a large number of MAC addresses through the network and fill up the available MAC address table space. You can control MAC address learning on a VLAN and manage the MAC address table space that is available on the switch by controlling which VLANs, and therefore which ports, can learn MAC addresses.

Before you disable MAC address learning, be sure that you are familiar with the network topology and the switch system configuration. Disabling MAC address learning on a VLAN could cause flooding in the network. See the “Disabling MAC Address Learning on a VLAN” section on page 5-29 for more information.

### Default MAC Address Table Configuration

Table 5-3 shows the default MAC address table configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aging time</td>
<td>300 seconds</td>
</tr>
<tr>
<td>Dynamic addresses</td>
<td>Automatically learned</td>
</tr>
<tr>
<td>Static addresses</td>
<td>None configured</td>
</tr>
<tr>
<td>MAC address learning on VLANs</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

### Changing the Address Aging Time

Dynamic addresses are source MAC addresses that the switch learns and then ages when they are not in use. You can change the aging time setting for all VLANs or for a specified VLAN.

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, which prevents new addresses from being learned. Flooding results, which can impact switch performance.
Beginning in privileged EXEC mode, follow these steps to configure the dynamic address table aging time:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> mac address-table aging-time [0</td>
<td>10-1000000] [vlan vlan-id]</td>
</tr>
<tr>
<td><strong>Step 3</strong> end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong> show mac address-table aging-time</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td><strong>Step 5</strong> copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default value, use the no mac address-table aging-time global configuration command.

### Removing Dynamic Address Entries

To remove all dynamic entries, use the clear mac address-table dynamic command in privileged EXEC mode. You can also remove a specific MAC address (clear mac address-table dynamic address mac-address), remove all addresses on the specified physical port or port channel (clear mac address-table dynamic interface interface-id), or remove all addresses on a specified VLAN (clear mac address-table dynamic vlan vlan-id).

To verify that dynamic entries have been removed, use the show mac address-table dynamic privileged EXEC command.

### Configuring MAC Address Change Notification Traps

MAC address change notification tracks users on a network by storing the MAC address change activity. When the switch learns or removes a MAC address, an SNMP notification trap can be sent to the NMS. If you have many users coming and going from the network, you can set a trap-interval time to bundle the notification traps to reduce network traffic. The MAC notification history table stores MAC address activity for each port for which the trap is set. MAC address change notifications are generated for dynamic and secure MAC addresses. Notifications are not generated for self addresses, multicast addresses, or other static addresses.
Beginning in privileged EXEC mode, follow these steps to configure the switch to send MAC address change notification traps to an NMS host:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>snmp-server host host-addr {traps</td>
<td>informs} {version {1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For host-addr, specify the name or address of the NMS.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Specify traps (the default) to send SNMP traps to the host. Specify informs to send SNMP informs to the host.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Specify the SNMP version to support. Version 1, the default, is not available with informs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For community-string, specify the string to send with the notification operation. Though you can set this string by using the snmp-server host command, we recommend that you define this string by using the snmp-server community command before using the snmp-server host command.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For notification-type, use the mac-notification keyword.</td>
</tr>
<tr>
<td>3</td>
<td>snmp-server enable traps mac-notification change</td>
<td>Enable the switch to send MAC address change notification traps to the NMS.</td>
</tr>
<tr>
<td>4</td>
<td>mac address-table notification change</td>
<td>Enable the MAC address change notification feature.</td>
</tr>
<tr>
<td>5</td>
<td>mac address-table notification change [interval value] [history-size value]</td>
<td>Enter the trap interval time and the history table size.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) For interval value, specify the notification trap interval in seconds between each set of traps that are generated to the NMS. The range is 0 to 2147483647 seconds; the default is 1 second.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) For history-size value, specify the maximum number of entries in the MAC notification history table. The range is 0 to 500; the default is 1.</td>
</tr>
<tr>
<td>6</td>
<td>interface interface-id</td>
<td>Enter interface configuration mode, and specify the Layer 2 interface on which to enable the SNMP MAC address notification trap.</td>
</tr>
<tr>
<td>7</td>
<td>snmp trap mac-notification change {added</td>
<td>removed}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enable the trap when a MAC address is added on this interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enable the trap when a MAC address is removed from this interface.</td>
</tr>
<tr>
<td>8</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
Managing the MAC Address Table

To disable MAC address-change notification traps, use the `no snmp-server enable traps mac-notification change` global configuration command. To disable the MAC address-change notification traps on a specific interface, use the `no snmp trap mac-notification change {added | removed}` interface configuration command. To disable the MAC address-change notification feature, use the `no mac address-table notification change` global configuration command.

This example shows how to specify 172.20.10.10 as the NMS, enable the switch to send MAC address notification traps to the NMS, enable the MAC address-change notification feature, set the interval time to 123 seconds, set the history-size to 100 entries, and enable traps whenever a MAC address is added on the specified port.

```
Switch(config)# snmp-server host 172.20.10.10 traps private mac-notification
Switch(config)# snmp-server enable traps mac-notification change
Switch(config)# mac address-table notification change
Switch(config)# mac address-table notification change interval 123
Switch(config)# mac address-table notification change history-size 100
Switch(config)# interface gigabitethernet1/1/2
Switch(config-if)# snmp trap mac-notification change added
```

You can verify your settings by entering the `show mac address-table notification change interface` and the `show mac address-table notification change` privileged EXEC commands.

### Configuring MAC Address Move Notification Traps

When you configure MAC-move notification, an SNMP notification is generated and sent to the network management system whenever a MAC address moves from one port to another within the same VLAN.
Beginning in privileged EXEC mode, follow these steps to configure the switch to send MAC address-move notification traps to an NMS host:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
</tbody>
</table>
| 2    | snmp-server host host-addr {traps | informs} {version {1 | 2c | 3}} community-string notification-type | Specify the recipient of the trap message.  
   - For host-addr, specify the name or address of the NMS.  
   - Specify traps (the default) to send SNMP traps to the host. Specify informs to send SNMP informs to the host.  
   - Specify the SNMP version to support. Version 1, the default, is not available with informs.  
   - For community-string, specify the string to send with the notification operation. Though you can set this string by using the snmp-server host command, we recommend that you define this string by using the snmp-server community command before using the snmp-server host command.  
   - For notification-type, use the mac-notification keyword. |
| 3    | snmp-server enable traps mac-notification move | Enable the switch to send MAC address move notification traps to the NMS. |
| 4    | mac address-table notification mac-move | Enable the MAC address move notification feature. |
| 5    | end | Return to privileged EXEC mode. |
| 6    | show mac address-table notification mac-move  
show running-config | Verify your entries. |
| 7    | copy running-config startup-config | (Optional) Save your entries in the configuration file. |

To disable MAC address-move notification traps, use the no snmp-server enable traps macro-notification move global configuration command. To disable the MAC address-move notification feature, use the no mac address-table notification mac-move global configuration command.

This example shows how to specify 172.20.10.10 as the NMS, enable the switch to send MAC address move notification traps to the NMS, enable the MAC address move notification feature, and enable traps when a MAC address moves from one port to another.

```
Switch(config)# snmp-server host 172.20.10.10 traps private mac-notification
Switch(config)# snmp-server enable traps mac-notification move
Switch(config)# mac address-table notification mac-move
```

You can verify your settings by entering the show mac address-table notification mac-move privileged EXEC commands.
Configuring MAC Threshold Notification Traps

When you configure MAC threshold notification, an SNMP notification is generated and sent to the network management system when a MAC address table threshold limit is reached or exceeded.

Beginning in privileged EXEC mode, follow these steps to configure the switch to send MAC address table threshold notification traps to an NMS host:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>`snmp-server host host-addr {traps</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>snmp-server enable traps mac-notification threshold</code></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>mac address-table notification threshold</code></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>`mac address-table notification threshold [limit percentage]</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>end</code></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><code>show mac address-table notification threshold</code></td>
</tr>
<tr>
<td></td>
<td><code>show running-config</code></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><code>copy running-config startup-config</code></td>
</tr>
</tbody>
</table>
To disable MAC address-threshold notification traps, use the `no snmp-server enable traps mac-notification threshold` global configuration command. To disable the MAC address-threshold notification feature, use the `no mac address-table notification threshold` global configuration command.

This example shows how to specify 172.20.10.10 as the NMS, enable the MAC address threshold notification feature, set the interval time to 123 seconds, and set the limit to 78 per cent.

Switch(config)# snmp-server host 172.20.10.10 traps private mac-notification
Switch(config)# snmp-server enable traps mac-notification threshold
Switch(config)# mac address-table notification threshold
Switch(config)# mac address-table notification threshold interval 123
Switch(config)# mac address-table notification threshold limit 78

You can verify your settings by entering the `show mac address-table notification threshold` privileged EXEC commands.

### Adding and Removing Static Address Entries

A static address has these characteristics:

- It is manually entered in the address table and must be manually removed.
- It can be a unicast address.
- It does not age and is retained when the switch restarts.

You can add and remove static addresses and define the forwarding behavior for them. The forwarding behavior determines 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 specify.

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.

You add a static address to the address table by specifying the destination MAC unicast address and the VLAN from which it is received. Packets received with this destination address are forwarded to the interface specified with the `interface-id` option.

When you configure a static MAC address in a private-VLAN primary or secondary VLAN, you should also configure the same static MAC address in all associated VLANs. Static MAC addresses configured in a private-VLAN primary or secondary VLAN are not replicated in the associated VLAN. For more information about private VLANs, see Chapter 13, “Configuring Private VLANs.”

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><code>mac address-table static mac-addr</code> <code>vlan vlan-id interface interface-id</code></td>
<td>Add a static address to the MAC address table.</td>
</tr>
<tr>
<td></td>
<td>- For <code>mac-addr</code>, specify the destination MAC unicast address to add to the address table. Packets with this destination address received in the specified VLAN are forwarded to the specified interface.</td>
</tr>
<tr>
<td></td>
<td>- For <code>vlan-id</code>, specify the VLAN for which the packet with the specified MAC address is received. The range is 1 to 4094.</td>
</tr>
<tr>
<td></td>
<td>- For <code>interface-id</code>, specify the interface to which the received packet is forwarded. Valid interfaces include physical ports.</td>
</tr>
</tbody>
</table>
Managing the MAC Address Table

To remove static entries from the address table, use the no mac address-table static mac-addr vlan vlan-id interface interface-id global configuration command.

This example shows how to add the static address c2f3.220a.12f4 to the MAC address table. When a packet is received in VLAN 4 with this MAC address as its destination address, the packet is forwarded to the specified interface:

```
Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 interface gigabitethernet1/0/1
```

**Configuring Unicast MAC Address Filtering**

When unicast MAC address filtering is enabled, the switch drops packets with specific source or destination MAC addresses. This feature is disabled by default and only supports unicast static addresses.

Follow these guidelines when using this feature:

- Multicast MAC addresses, broadcast MAC addresses, and router MAC addresses are not supported. If you specify one of these addresses when entering the mac address-table static mac-addr vlan vlan-id drop global configuration command, one of these messages appears:
  ```
  % Only unicast addresses can be configured to be dropped
  % CPU destined address cannot be configured as drop address
  ```

- Packets that are forwarded to the CPU are also not supported.

- If you add a unicast MAC address as a static address and configure unicast MAC address filtering, the switch either adds the MAC address as a static address or drops packets with that MAC address, depending on which command was entered last. The second command that you entered overrides the first command.

For example, if you enter the mac address-table static mac-addr vlan vlan-id interface interface-id global configuration command followed by the mac address-table static mac-addr vlan vlan-id drop command, the switch drops packets with the specified MAC address as a source or destination.

If you enter the mac address-table static mac-addr vlan vlan-id drop global configuration command followed by the mac address-table static mac-addr vlan vlan-id interface interface-id command, the switch adds the MAC address as a static address.

You enable unicast MAC address filtering and configure the switch to drop packets with a specific address by specifying the source or destination unicast MAC address and the VLAN from which it is received.
Beginning in privileged EXEC mode, follow these steps to configure the switch to drop a source or destination unicast static address:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>mac address-table static mac-addr vlan vlan-id drop</td>
</tr>
<tr>
<td></td>
<td>Enable unicast MAC address filtering and configure the switch to drop a packet with the specified source or destination unicast static address.</td>
</tr>
<tr>
<td></td>
<td>- For mac-addr, specify a source or destination unicast MAC address. Packets with this MAC address are dropped.</td>
</tr>
<tr>
<td></td>
<td>- For vlan-id, specify the VLAN for which the packet with the specified MAC address is received. Valid VLAN IDs are 1 to 4094.</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
</tr>
<tr>
<td></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show mac address-table static</td>
</tr>
<tr>
<td></td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 5</td>
<td>copy running-config startup-config</td>
</tr>
<tr>
<td></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable unicast MAC address filtering, use the **no mac address-table static mac-addr vlan vlan-id** global configuration command.

This example shows how to enable unicast MAC address filtering and to configure the switch to drop packets that have a source or destination address of c2f3.220a.12f4. When a packet is received in VLAN 4 with this MAC address as its source or destination, the packet is dropped:

```
Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 drop
```

**Disabling MAC Address Learning on a VLAN**

By default, MAC address learning is enabled on all VLANs on the switch. You can control MAC address learning on a VLAN to manage the available MAC address table space by controlling which VLANs, and therefore which ports, can learn MAC addresses. Before you disable MAC address learning be sure that you are familiar with the network topology and the switch system configuration. Disabling MAC address learning on a VLAN could cause flooding in the network.

Follow these guidelines when disabling MAC address learning on a VLAN:

- Use caution before disabling MAC address learning on a VLAN with a configured switch virtual interface (SVI). The switch then floods all IP packets in the Layer 2 domain.

- You can disable MAC address learning on a single VLAN (for example, **no mac address-table learning vlan 223**) or on a range of VLANs (for example, **no mac address-table learning vlan 1-10, 15**).

- We recommend that you disable MAC address learning only in VLANs with two ports. If you disable MAC address learning on a VLAN with more than two ports, every packet entering the switch is flooded in that VLAN domain.

- You cannot disable MAC address learning on a VLAN that is used internally by the switch. If the VLAN ID that you enter is an internal VLAN, the switch generates an error message and rejects the command. To view internal VLANs in use, enter the **show vlan internal usage** privileged EXEC command.
If you disable MAC address learning on a VLAN configured as a private-VLAN primary VLAN, MAC addresses are still learned on the secondary VLAN that belongs to the private VLAN and are then replicated on the primary VLAN. If you disable MAC address learning on the secondary VLAN, but not the primary VLAN of a private VLAN, MAC address learning occurs on the primary VLAN and is replicated on the secondary VLAN.

You cannot disable MAC address learning on an RSPAN VLAN. The configuration is not allowed.

If you disable MAC address learning on a VLAN that includes a secure port, MAC address learning is not disabled on that port. If you disable port security, the configured MAC address learning state is enabled.

Beginning in privileged EXEC mode, follow these steps to disable MAC address learning on a VLAN:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>no mac address-table learning vlan vlan-id</td>
<td>Disable MAC address learning on the specified VLAN or VLANs. You can specify a single VLAN or a range of VLANs separated by a hyphen or comma. Valid VLAN IDs are 1 to 4094. The VLAN cannot be an internal VLAN.</td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>show mac address-table learning [vlan vlan-id]</td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To re-enable MAC address learning on a VLAN, use the default mac address-table learning vlan vlan-id global configuration command. You can also reenable MAC address learning on a VLAN by entering the mac address-table learning vlan vlan-id global configuration command. The first (default) command returns to a default condition and therefore does not appear in the output from the show running-config privileged EXEC command display.

This example shows how to disable MAC address learning on VLAN 200:

```
Switch(config)# no mac address-table learning vlan 200
```

You can display the MAC address learning status of all VLANs or a specified VLAN by entering the show mac-address-table learning [vlan vlan-id] privileged EXEC command.

### Displaying Address Table Entries

You can display the MAC address table by using one or more of the privileged EXEC commands described in Table 5-4:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mac address-table address</td>
<td>Displays MAC address table information for the specified MAC address.</td>
</tr>
<tr>
<td>show mac address-table aging-time</td>
<td>Displays the aging time in all VLANs or the specified VLAN.</td>
</tr>
<tr>
<td>show mac address-table count</td>
<td>Displays the number of addresses present in all VLANs or the specified VLAN.</td>
</tr>
</tbody>
</table>
Managing the ARP Table

To communicate with a device (over Ethernet, for example), the software first must determine the 48-bit MAC or the 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 the 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.

ARP entries added manually to the table do not age and must be manually removed.

For more information, see the Cisco IOS Release 12.2 documentation on Cisco.com.

### Table 5-4 Commands for Displaying the MAC Address Table (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>show mac address-table dynamic</strong></td>
<td>Displays only dynamic MAC address table entries.</td>
</tr>
<tr>
<td><strong>show mac address-table interface</strong></td>
<td>Displays the MAC address table information for the specified interface.</td>
</tr>
<tr>
<td><strong>show mac address-table learning</strong></td>
<td>Displays MAC address learning status of all VLANs or the specified VLAN.</td>
</tr>
<tr>
<td><strong>show mac address-table multicast</strong></td>
<td>Displays the Layer 2 multicast entries for all VLANs or the specified VLAN.</td>
</tr>
<tr>
<td><strong>show mac address-table notification</strong></td>
<td>Displays the MAC notification parameters and history table.</td>
</tr>
<tr>
<td><strong>show mac address-table static</strong></td>
<td>Displays only static MAC address table entries.</td>
</tr>
<tr>
<td><strong>show mac address-table vlan</strong></td>
<td>Displays the MAC address table information for the specified VLAN.</td>
</tr>
</tbody>
</table>
Configuring SDM Templates

This chapter describes how to configure the Switch Database Management (SDM) templates on the Catalyst 3750 Metro switch.

Note

For complete syntax and usage information for the commands used in this chapter, see the command reference for this release.

This chapter consists of these sections:
- Understanding the SDM Templates, page 6-1
- Configuring the Switch SDM Template, page 6-3
- Displaying the SDM Templates, page 6-5

Understanding the SDM Templates

You can use SDM templates to configure system resources in the switch to optimize support for specific features, depending on how the switch is used in the network. You can use the SDM templates for IP Version 4 (IPv4) and select a template to provide maximum system usage for some functions or to use the default template to balance resources.

The templates prioritize system resources to optimize support for these types of features:
- Routing—The routing template maximizes system resources for unicast routing, typically required for a router or aggregator in the center of a network.
- VLANs—The VLAN template disables routing and supports the maximum number of unicast MAC addresses. It would typically be selected for a Layer 2 switch.
- Default—The default template gives balance to all functions.

The dual IPv4 and IPv6 templates also enable a dual stack environment. See the “Dual IPv4 and IPv6 SDM Templates” section on page 6-2.

Table 6-1 lists the approximate numbers of each resource supported in each of the three supported IPv4 templates.
Understanding the SDM Templates

The first eight rows in the tables (unicast MAC addresses through security ACEs) represent approximate hardware boundaries set when a template is selected. If a section of a hardware resource is full, all processing overflow is sent to the CPU, seriously impacting switch performance. The last row is a guideline used to calculate hardware resource consumption related to the number of Layer 2 VLANs on the switch.

### Table 6-1 Approximate Number of Feature Resources Allowed by Each Template

<table>
<thead>
<tr>
<th>Resource</th>
<th>Template</th>
<th>Default</th>
<th>Routing</th>
<th>VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unicast MAC addresses</td>
<td></td>
<td>6 K</td>
<td>3 K</td>
<td>12 K</td>
</tr>
<tr>
<td>IGMP groups and multicast routes</td>
<td></td>
<td>1 K</td>
<td>1 K</td>
<td>1 K</td>
</tr>
<tr>
<td>Unicast routes</td>
<td></td>
<td>8 K</td>
<td>11 K</td>
<td>0</td>
</tr>
<tr>
<td>• Directly connected hosts</td>
<td></td>
<td>6 K</td>
<td>3 K</td>
<td>0</td>
</tr>
<tr>
<td>• Indirect routes</td>
<td></td>
<td>2 K</td>
<td>8 K</td>
<td>0</td>
</tr>
<tr>
<td>Policy-based routing ACEs</td>
<td></td>
<td>0</td>
<td>512</td>
<td>0</td>
</tr>
<tr>
<td>QoS classification ACEs</td>
<td></td>
<td>512</td>
<td>512</td>
<td>512</td>
</tr>
<tr>
<td>Security ACEs</td>
<td></td>
<td>1 K</td>
<td>1 K</td>
<td>1 K</td>
</tr>
<tr>
<td>Layer 2 VLANs</td>
<td></td>
<td>1 K</td>
<td>1 K</td>
<td>1 K</td>
</tr>
</tbody>
</table>

The dual IPv4 and IPv6 SDM Templates

You can select SDM templates to support IP Version 6 (IPv6). For more information about IPv6 and how to configure IPv6 routing, see Chapter 37, “Configuring IPv6 Unicast Routing.” For information about IPv6 MLD snooping, see Chapter 38, “Configuring IPv6 MLD Snooping.” For information about configuring IPv6 ACLs, see Chapter 39, “Configuring IPv6 ACLs.”

This software release does not support Policy-Based Routing (PBR) when forwarding IPv6 traffic. The software supports IPv4 PBR only when the `dual-ipv4-and-ipv6 routing` template is configured.

The dual IPv4 and IPv6 templates allow the switch to be used in dual stack environments (supporting both IPv4 and IPv6). Using the dual stack templates results in less TCAM capacity allowed for each resource. Do not use them if you plan to forward only IPv4 traffic.

These SDM templates support IPv4 and IPv6 environments:

- Dual IPv4 and IPv6 default template—supports Layer 2, multicast, routing, QoS, and ACLs for IPv4; and Layer 2, routing, and ACLs for IPv6 on the switch.
- Dual IPv4 and IPv6 routing template—supports Layer 2, multicast, routing (including policy-based routing), QoS, and ACLs for IPv4; and Layer 2, routing, and ACLs for IPv6 on the switch.
- Dual IPv4 and IPv6 VLAN template—supports basic Layer 2, multicast, QoS, and ACLs for IPv4, and basic Layer 2 and ACLs for IPv6 on the switch.

This software release does not support IPv6 multicast routing or IPv6 QoS.

**Note** An IPv4 route requires only one TCAM entry. Because of the hardware compression scheme used for IPv6, an IPv6 route can take more than one TCAM entry, reducing the number of entries forwarded in hardware.
Table 7-2 defines the approximate feature resources allocated by each dual template. Template estimations are based on a switch with 8 routed interfaces and approximately 1000 VLANs.

Table 6-2 Approximate Feature Resources Allowed by Dual IPv4-IPv6 Templates

<table>
<thead>
<tr>
<th>Resource</th>
<th>Default</th>
<th>Routing</th>
<th>VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unicast MAC addresses</td>
<td>2 K</td>
<td>1536</td>
<td>8 K</td>
</tr>
<tr>
<td>IPv4 IGMP groups and multicast routes</td>
<td>1 K</td>
<td>1 K</td>
<td>1 K</td>
</tr>
<tr>
<td>Total IPv4 unicast routes:</td>
<td>3 K</td>
<td>2816</td>
<td>0</td>
</tr>
<tr>
<td>• Directly connected IPv4 hosts</td>
<td>2 K</td>
<td>1536</td>
<td>0</td>
</tr>
<tr>
<td>• Indirect IPv4 routes</td>
<td>1 K</td>
<td>1280</td>
<td>0</td>
</tr>
<tr>
<td>IPv6 multicast groups</td>
<td>1 K</td>
<td>1152</td>
<td>1 K</td>
</tr>
<tr>
<td>Total IPv6 unicast routes:</td>
<td>3 K</td>
<td>2816</td>
<td>0</td>
</tr>
<tr>
<td>• Directly connected IPv6 addresses</td>
<td>2 K</td>
<td>1536</td>
<td>0</td>
</tr>
<tr>
<td>• Indirect IPv6 unicast routes</td>
<td>1 K</td>
<td>1280</td>
<td>0</td>
</tr>
<tr>
<td>IPv4 policy-based routing ACEs</td>
<td>0</td>
<td>256</td>
<td>0</td>
</tr>
<tr>
<td>IPv4 or MAC QoS ACEs (total)</td>
<td>512</td>
<td>512</td>
<td>512</td>
</tr>
<tr>
<td>IPv4 or MAC security ACEs (total)</td>
<td>1 K</td>
<td>512</td>
<td>1 K</td>
</tr>
<tr>
<td>IPv6 policy-based routing ACEs¹</td>
<td>0</td>
<td>255</td>
<td>0</td>
</tr>
<tr>
<td>IPv6 QoS ACEs</td>
<td>510</td>
<td>510</td>
<td>510</td>
</tr>
<tr>
<td>IPv6 security ACEs</td>
<td>510</td>
<td>510</td>
<td>510</td>
</tr>
</tbody>
</table>

1. IPv6 policy-based routing is not supported in this release.

Configuring the Switch SDM Template

This section describes how to configure the SDM template to be used on the switch. This section contains this configuration information:

- Default SDM Template, page 6-3
- SDM Template Configuration Guidelines, page 6-4
- Setting the SDM Template, page 6-4

Default SDM Template

The default template is the default (nondual) template.
SDM Template Configuration Guidelines

Follow these guidelines when selecting and configuring SDM templates:

- You must reload the switch for the configuration to take effect.
- Use the `sdm prefer vlan` global configuration command only on switches intended for Layer 2 switching with no routing. When you use the VLAN template, no system resources are reserved for routing entries, and any routing is done through software. This overloads the CPU and severely degrades routing performance.
- Do not use the routing template if you do not have routing enabled on your switch. The `sdm prefer routing` global configuration command prevents other features from using the memory allocated to unicast routing in the routing template.
- If you try to configure IPv6 features without first selecting a dual IPv4 and IPv6 template, a warning message appears.
- Using the dual-stack templates results in less TCAM capacity allowed for each resource. Do not use them if you plan to forward only IPv4 traffic.

Setting the SDM Template

Beginning in privileged EXEC mode, follow these steps to use the SDM template to maximize resources:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>sdm prefer {default</td>
</tr>
<tr>
<td></td>
<td>(default</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
</tr>
<tr>
<td>Step 4</td>
<td>reload</td>
</tr>
</tbody>
</table>

After the system reboots, you can use the `show sdm prefer` privileged EXEC command to verify the new template configuration. If you enter the `show sdm prefer` command before you enter the `reload` privileged EXEC command, the `show sdm prefer` command shows the template currently in use and the template that will become active after a reload.
This is an example of an output display when you have changed the template and have not reloaded the switch:

Switch# `show sdm prefer`  
The current template is "desktop routing" template.  
The selected template optimizes the resources in  
the switch to support this level of features for  
8 routed interfaces and 1024 VLANs.  

number of unicast mac addresses: 3K  
number of igmp groups + multicast routes: 1K  
number of unicast routes: 11K  
number of directly connected hosts: 3K  
number of indirect routes: 8K  
number of qos aces: 512  
number of security aces: 1K

On next reload, template will be 'desktop vlan' template.  

To return to the default template, use the `no sdm prefer` global configuration command.  

This example shows how to configure a switch with the routing template.  

Switch(config)# `sdm prefer routing`  
Switch(config)# `end`  
Switch# `reload`  
Proceed with reload? [confirm]

**Displaying the SDM Templates**

Use the `show sdm prefer` privileged EXEC command with no parameters to display the active template.  

Use the `show sdm prefer [default | dual-ipv4-and-ipv6 | default | routing | vlan] routing | vlan` privileged EXEC command to display the resource numbers supported by the specified template.  

This is an example of output from the `show sdm prefer` command, displaying the template in use.  

Switch# `show sdm prefer`  
The current template is "desktop default" template.  
The selected template optimizes the resources in  
the switch to support this level of features for  
8 routed interfaces and 1024 VLANs.  

number of unicast mac addresses: 6K  
number of igmp groups + multicast routes: 1K  
number of unicast routes: 8K  
number of directly connected hosts: 6K  
number of indirect routes: 2K  
number of policy based routing aces: 0  
number of qos aces: 512  
number of security aces: 1K

This is an example of output from the `show sdm prefer routing` command:

Switch# `show sdm prefer routing`  
"desktop routing" template:  
The selected template optimizes the resources in  
the switch to support this level of features for  
8 routed interfaces and 1024 VLANs.  

number of unicast mac addresses: 3K  
number of igmp groups + multicast routes: 1K  
number of unicast routes: 11K
number of directly connected hosts: 3K
number of indirect routes: 8K
number of policy based routing aces: 512
number of qos aces: 512
number of security aces: 1K

This is an example of output from the `show sdm prefer dual-ipv4-and-ipv6 default` command entered on a switch:

```
Switch# show sdm prefer dual-ipv4-and-ipv6 default
desktop IPv4 and IPv6 default' template:
The selected template optimizes the resources in the switch to support this level of features for 8 routed interfaces and 1024 VLANs.

number of unicast mac addresses: 2K
number of IPv4 IGMP groups + multicast routes: 1K
number of IPv4 unicast routes: 3K
  number of directly-connected IPv4 hosts: 2K
  number of indirect IPv4 routes: 1K
number of IPv6 multicast groups: 1K
number of directly-connected IPv6 addresses: 2K
number of indirect IPv6 unicast routes: 1K
number of IPv4 policy based routing aces: 0
number of IPv4/MAC qos aces: 0.5K
number of IPv4/MAC security aces: 1K
number of IPv6 policy based routing aces: 0
number of IPv6 qos aces: 0.5K
number of IPv6 security aces: 0.5K
```
CHAPTER 7

Configuring Switch-Based Authentication

This chapter describes how to configure switch-based authentication on the Catalyst 3750 Metro switch. It consists of these sections:

- Preventing Unauthorized Access to Your Switch, page 7-1
- Protecting Access to Privileged EXEC Commands, page 7-2
- Controlling Switch Access with TACACS+, page 7-9
- Controlling Switch Access with RADIUS, page 7-16
- Controlling Switch Access with Kerberos, page 7-31
- Configuring the Switch for Local Authentication and Authorization, page 7-35
- Configuring the Switch for Secure Shell, page 7-36
- Configuring the Switch for Secure Socket Layer HTTP, page 7-40
- Configuring the Switch for Secure Copy Protocol, page 7-46

Preventing Unauthorized Access to Your Switch

You can prevent unauthorized users from reconfiguring your switch and viewing configuration information. Typically, you want network administrators to have access to your switch while you restrict access to users who dial from outside the network through an asynchronous port, connect from outside the network through a serial port, or connect through a terminal or workstation from within the local network.

To prevent unauthorized access into your switch, you should configure one or more of these security features:

- At a minimum, you should configure passwords and privileges at each switch port. These passwords are locally stored on the switch. When users attempt to access the switch through a port or line, they must enter the password specified for the port or line before they can access the switch. For more information, see the “Protecting Access to Privileged EXEC Commands” section on page 7-2.
- For an additional layer of security, you can also configure username and password pairs, which are locally stored on the switch. These pairs are assigned to lines or ports and authenticate each user before that user can access the switch. If you have defined privilege levels, you can also assign a specific privilege level (with associated rights and privileges) to each username and password pair. For more information, see the “Configuring Username and Password Pairs” section on page 7-6.
If you want to use username and password pairs, but you want to store them centrally on a server instead of locally, you can store them in a database on a security server. Multiple networking devices can then use the same database to obtain user authentication (and, if necessary, authorization) information. For more information, see the “Controlling Switch Access with TACACS+” section on page 7-9.

### Protecting Access to Privileged EXEC Commands

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

**Note**

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

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

- Default Password and Privilege Level Configuration, page 7-2
- Setting or Changing a Static Enable Password, page 7-3
- Protecting Enable and Enable Secret Passwords with Encryption, page 7-3
- Disabling Password Recovery, page 7-5
- Setting a Telnet Password for a Terminal Line, page 7-6
- Configuring Username and Password Pairs, page 7-6
- Configuring Multiple Privilege Levels, page 7-7

### Default Password and Privilege Level Configuration

*Table 7-1* shows the default password and privilege level configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable password and privilege level</td>
<td>No password is defined. The default is level 15 (privileged EXEC level).</td>
</tr>
<tr>
<td></td>
<td>The password is not encrypted in the configuration file.</td>
</tr>
<tr>
<td>Enable secret password and privilege level</td>
<td>No password is defined. The default is level 15 (privileged EXEC level).</td>
</tr>
<tr>
<td></td>
<td>The password is encrypted before it is written to the configuration file.</td>
</tr>
<tr>
<td>Line password</td>
<td>No password is defined.</td>
</tr>
</tbody>
</table>
Setting or Changing a Static Enable Password

The enable password controls access to the privileged EXEC mode. Beginning in privileged EXEC mode, follow these steps to set or change a static enable password:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>enable password <em>password</em></td>
<td>Define a new password or change an existing password for access to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>By default, no password is defined.</td>
</tr>
<tr>
<td></td>
<td>For <em>password</em>, specify a string from 1 to 25 alphanumeric characters.</td>
</tr>
<tr>
<td></td>
<td>The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces. It can contain the question mark (?) character if you precede the question mark with the key combination Ctrl-v when you create the password; for example, to create the password abc?123, do this:</td>
</tr>
<tr>
<td></td>
<td>Enter abc.</td>
</tr>
<tr>
<td></td>
<td>Enter Ctrl-v.</td>
</tr>
<tr>
<td></td>
<td>Enter ?123.</td>
</tr>
<tr>
<td></td>
<td>When the system prompts you to enter the enable password, you need not precede the question mark with the Ctrl-v; you can simply enter abc?123 at the password prompt.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
<tr>
<td></td>
<td>The enable password is not encrypted and can be read in the switch configuration file.</td>
</tr>
</tbody>
</table>

To remove the password, use the no enable password global configuration command.

This example shows how to change the enable password to 1lu2c3k4y5. The password is not encrypted and provides access to level 15 (traditional privileged EXEC mode access):

```
Switch(config)# enable password 1lu2c3k4y5
```

Protecting Enable and Enable Secret Passwords with Encryption

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

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

If you configure the enable secret command, it takes precedence over the enable password command; the two commands cannot be in effect simultaneously.
Beginning in privileged EXEC mode, follow these steps to configure encryption for enable and enable secret passwords:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>enable password [level level] {password \ encryption-type encrypted-password}</td>
<td>Define a new password or change an existing password for access to privileged EXEC mode.</td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td>enable secret [level level] {password \ encryption-type encrypted-password}</td>
<td>Define a secret password, which is saved using a nonreversible encryption method.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>(Optional) Encrypt the password when the password is defined or when the configuration is written. Encryption prevents the password from being readable in the configuration file.</td>
</tr>
<tr>
<td>service password-encryption</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

If both the enable and enable secret passwords are defined, users must enter the enable secret password. Use the level keyword to define a password for a specific privilege level. After you specify the level and set a password, give the password only to users who need to have access at this level. Use the privilege level global configuration command to specify commands accessible at various levels. For more information, see the “Configuring Multiple Privilege Levels” section on page 7-7.

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

To remove a password and level, use the no enable password [level level] or no enable secret [level level] global configuration command. To disable password encryption, use the no service password-encryption global configuration command.
This example shows how to configure the encrypted password `$1$FaD0$Xyti5Rkls3LoyxzS8` for privilege level 2:

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

## Disabling Password Recovery

By default, any end user with physical access to the switch can recover from a lost password by interrupting the boot process while the switch is powering on and then by entering a new password.

The password-recovery disable feature protects access to the switch password by disabling part of this functionality. When this feature is enabled, the end user can interrupt the boot process only by agreeing to set the system back to the default configuration. With password recovery disabled, you can still interrupt the boot process and change the password, but the configuration file (`config.text`) and the VLAN database file (`vlan.dat`) are deleted.

**Note**

If you disable password recovery, we recommend that you keep a backup copy of the configuration file on a secure server in case the end user interrupts the boot process and sets the system back to default values. Do not keep a backup copy of the configuration file on the switch. If the switch is operating in VTP transparent mode, we recommend that you also keep a backup copy of the VLAN database file on a secure server. When the switch is returned to the default system configuration, you can download the saved files to the switch by using the Xmodem protocol. For more information, see the “Recovering from a Lost or Forgotten Password” section on page 48-3.

Beginning in privileged EXEC mode, follow these steps to disable password recovery:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>no service password-recovery</td>
<td>Disable password recovery. This setting is saved in an area of the flash memory that is accessible by the boot loader and the Cisco IOS image, but it is not part of the file system and is not accessible by any user.</td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>show version</td>
<td>Verify the configuration by checking the last few lines of the display.</td>
</tr>
</tbody>
</table>

To re-enable password recovery, use the `service password-recovery` global configuration command.

**Note**

Disabling password recovery does not work if you have set the switch to boot manually by using the `boot manual` global configuration command. This command produces the boot loader prompt (`switch:`) after the switch is power cycled.
Chapter 7 Configuring Switch-Based Authentication

Setting a Telnet Password for a Terminal Line

When you power-up your switch for the first time, an automatic setup program runs to assign IP information and to create a default configuration for continued use. The setup program also prompts you to configure your switch for Telnet access through a password. If you did not configure this password during the setup program, you can configure it now through the command-line interface (CLI).

Beginning in privileged EXEC mode, follow these steps to configure your switch for Telnet access:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | Attach a PC or workstation with emulation software to the switch console port. 
The default data characteristics of the console port are 9600, 8, 1, no parity. You might need to press the Return key several times to see the command-line prompt. |
| Step 2 | enable password password Enter privileged EXEC mode. |
| Step 3 | configure terminal Enter global configuration mode. |
| Step 4 | line vty 0 15 Configure the number of Telnet sessions (lines), and enter line configuration mode. 
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 | password password Enter a Telnet password for the line or lines. 
For password, specify a string from 1 to 25 alphanumeric characters. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces. By default, no password is defined. |
| Step 6 | end Return to privileged EXEC mode. |
| Step 7 | show running-config Verify your entries. 
The password is listed under the command line vty 0 15. |
| Step 8 | copy running-config startup-config (Optional) Save your entries in the configuration file. |

To remove the password, use the no password global configuration command.

This example shows how to set the Telnet password to let45me67in89:

```
Switch(config)# line vty 10
Switch(config-line)# password let45me67in89
```

Configuring Username and Password Pairs

You can configure username and password pairs, which are locally stored on the switch. These pairs are assigned to lines or ports and authenticate each user before that user can access the switch. If you have defined privilege levels, you can also assign a specific privilege level (with associated rights and privileges) to each username and password pair.
Beginning in privileged EXEC mode, follow these steps to establish a username-based authentication system that requests a login username and a password:

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

To disable username authentication for a specific user, use the no username name global configuration command. To disable password checking and allow connections without a password, use the no login global configuration command.

**Configuring Multiple Privilege Levels**

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

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

This section includes this configuration information:
- Setting the Privilege Level for a Command, page 7-8
- Changing the Default Privilege Level for Lines, page 7-9
- Logging into and Exiting a Privilege Level, page 7-9
Setting the Privilege Level for a Command

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

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

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

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

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

```
Switch(config)# privilege exec level 14 configure
Switch(config)# enable password level 14 SecretPswd14
```
Changing the Default Privilege Level for Lines

Beginning in privileged EXEC mode, follow these steps to change the default privilege level for a line:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>line vty line</td>
<td>Select the virtual terminal line on which to restrict access.</td>
</tr>
<tr>
<td>privilege level level</td>
<td>Change the default privilege level for the line.</td>
</tr>
<tr>
<td></td>
<td>For level, the range is from 0 to 15. Level 1 is for normal user EXEC</td>
</tr>
<tr>
<td></td>
<td>mode privileges. Level 15 is the level of access permitted by the enable</td>
</tr>
<tr>
<td></td>
<td>password.</td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>or</td>
<td>The first command displays the password and access level configuration.</td>
</tr>
<tr>
<td>show privilege</td>
<td>The second command displays the privilege level configuration.</td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Users can override the privilege level you set using the privilege level line configuration command by logging in to the line and enabling a different privilege level. They can lower the privilege level by using the disable command. If users know the password to a higher privilege level, they can use that password to enable the higher privilege level. You might specify a high level or privilege level for your console line to restrict line usage.

To return to the default line privilege level, use the no privilege level line configuration command.

Logging into and Exiting a Privilege Level

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable level</td>
<td>Log in to a specified privilege level.</td>
</tr>
<tr>
<td></td>
<td>For level, the range is 0 to 15.</td>
</tr>
<tr>
<td>disable level</td>
<td>Exit to a specified privilege level.</td>
</tr>
<tr>
<td></td>
<td>For level, the range is 0 to 15.</td>
</tr>
</tbody>
</table>

Controlling Switch Access with TACACS+

This section describes how to enable and configure TACACS+, which provides detailed accounting information and flexible administrative control over authentication and authorization processes. TACACS+ is facilitated through authentication, authorization, accounting (AAA) and can be enabled only through AAA commands.
Note

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

This section contains this configuration information:

- **Understanding TACACS+**, page 7-10
- **TACACS+ Operation**, page 7-11
- **Configuring TACACS+**, page 7-12
- **Displaying the TACACS+ Configuration**, page 7-16

## Understanding TACACS+

TACACS+ is a security application that provides centralized validation of users attempting to gain access to your switch. TACACS+ services are maintained in a database on a TACACS+ daemon typically running on a UNIX or Windows NT workstation. You should have access to and should configure a TACACS+ server before the configuring TACACS+ features on your switch.

TACACS+ provides for separate and modular authentication, authorization, and accounting facilities. TACACS+ allows for a single access control server (the TACACS+ daemon) to provide each service—authentication, authorization, and accounting—independently. Each service can be tied into its own database to take advantage of other services available on that server or on the network, depending on the capabilities of the daemon.

The goal of TACACS+ is to provide a method for managing multiple network access points from a single management service. Your switch can be a network access server along with other Cisco routers and access servers. A network access server provides connections to a single user, to a network or subnetwork, and to interconnected networks as shown in Figure 7-1.

### Figure 7-1  Typical TACACS+ Network Configuration

![Typical TACACS+ Network Configuration Diagram](image)
TACACS+, administered through the AAA security services, can provide these services:

- **Authentication**—Provides complete control of authentication through login and password dialog, challenge and response, and messaging support.

  The authentication facility can conduct a dialog with the user (for example, after a username and password are provided, to challenge a user with several questions, such as home address, mother’s maiden name, service type, and social security number). The TACACS+ authentication service can also send messages to user screens. For example, a message could notify users that their passwords must be changed because of the company’s password aging policy.

- **Authorization**—Provides fine-grained control over user capabilities for the duration of the user’s session, including but not limited to setting autocommands, access control, session duration, or protocol support. You can also enforce restrictions on what commands a user can execute with the TACACS+ authorization feature.

- **Accounting**—Collects and sends information used for billing, auditing, and reporting to the TACACS+ daemon. Network managers can use the accounting facility to track user activity for a security audit or to provide information for user billing. Accounting records include user identities, start and stop times, executed commands (such as PPP), number of packets, and number of bytes.

The TACACS+ protocol provides authentication between the switch and the TACACS+ daemon, and it ensures confidentiality because all protocol exchanges between the switch and the TACACS+ daemon are encrypted.

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

## TACACS+ Operation

When a user attempts a simple ASCII login by authenticating to a switch using TACACS+, this process occurs:

1. **When the connection is established, the switch contacts the TACACS+ daemon to obtain a username prompt, which is then displayed to the user. The user enters a username, and the switch then contacts the TACACS+ daemon to obtain a password prompt. The switch displays the password prompt to the user, the user enters a password, and the password is then sent to the TACACS+ daemon.**

   TACACS+ allows a conversation to be held between the daemon and the user until the daemon receives enough information to authenticate the user. The daemon prompts for a username and password combination, but can include other items, such as the user’s mother’s maiden name.

2. **The switch eventually receives one of these responses from the TACACS+ daemon:**
   - **ACCEPT**—The user is authenticated and service can begin. If the switch is configured to require authorization, authorization begins at this time.
   - **REJECT**—The user is not authenticated. The user can be denied access or is prompted to retry the login sequence, depending on the TACACS+ daemon.
   - **ERROR**—An error occurred at some time during authentication with the daemon or in the network connection between the daemon and the switch. If an ERROR response is received, the switch typically tries to use an alternative method for authenticating the user.
   - **CONTINUE**—The user is prompted for additional authentication information.

After authentication, the user undergoes an additional authorization phase if authorization has been enabled on the switch. Users must first successfully complete TACACS+ authentication before proceeding to TACACS+ authorization.
3. If TACACS+ authorization is required, the TACACS+ daemon is again contacted, and it returns an ACCEPT or REJECT authorization response. If an ACCEPT response is returned, the response contains data in the form of attributes that direct the EXEC or NETWORK session for that user and the services that the user can access:
   
   - Telnet, Secure Shell (SSH), rlogin, or privileged EXEC services
   - Connection parameters, including the host or client IP address, access list, and user timeouts

**Configuring TACACS+**

This section describes how to configure your switch to support TACACS+. At a minimum, you must identify the host or hosts maintaining the TACACS+ daemon and define the method lists for TACACS+ authentication. You can optionally define method lists for TACACS+ authorization and accounting. A method list defines the sequence and methods to be used to authenticate, to authorize, or to keep accounts on a user. You can use method lists to designate one or more security protocols to be used, thus ensuring a backup system if the initial method fails. The software uses the first method listed to authenticate, to authorize, or to keep accounts on users; if that method does not respond, the software selects the next method in the list. This process continues until there is successful communication with a listed method or the method list is exhausted.

This section contains this configuration information:

- Default TACACS+ Configuration, page 7-12
- Identifying the TACACS+ Server Host and Setting the Authentication Key, page 7-12
- Configuring TACACS+ Login Authentication, page 7-13
- Configuring TACACS+ Authorization for Privileged EXEC Access and Network Services, page 7-15
- Starting TACACS+ Accounting, page 7-16

**Default TACACS+ Configuration**

TACACS+ and AAA are disabled by default.

To prevent a lapse in security, you cannot configure TACACS+ through a network management application. When enabled, TACACS+ can authenticate users accessing the switch through the CLI.

**Note**

Although TACACS+ configuration is performed through the CLI, the TACACS+ server authenticates HTTP connections that have been configured with a privilege level of 15.

**Identifying the TACACS+ Server Host and Setting the Authentication Key**

You can configure the switch to use a single server or AAA server groups to group existing server hosts for authentication. You can group servers to select a subset of the configured server hosts and use them for a particular service. The server group is used with a global server-host list and contains the list of IP addresses of the selected server hosts.

Beginning in privileged EXEC mode, follow these steps to identify the IP host or host maintaining TACACS+ server and optionally set the encryption key:
Chapter 7 Configuring Switch-Based Authentication

Controlling Switch Access with TACACS+

To remove the specified TACACS+ server name or address, use the `no tacacs-server host hostname` global configuration command. To remove a server group from the configuration list, use the `no aaa group server tacacs+ group-name` global configuration command. To remove the IP address of a TACACS+ server, use the `no server ip-address` server group subconfiguration command.

### Configuring TACACS+ Login Authentication

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

A method list describes the sequence and authentication methods to be queried to authenticate a user. You can designate one or more security protocols to be used for authentication, thus ensuring a backup system for authentication in case the initial method fails. The software uses the first method listed to authenticate users; if that method fails to respond, the software selects the next authentication method in the method list. This process continues until there is successful communication with a listed

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><code>tacacs-server host hostname [port integer] [timeout integer] [key string]</code></td>
<td>Identify the IP host or hosts maintaining a TACACS+ server. Enter this command multiple times to create a list of preferred hosts. The software searches for hosts in the order in which you specify them.</td>
</tr>
<tr>
<td>· For <code>hostname</code>, specify the name or IP address of the host.</td>
<td></td>
</tr>
<tr>
<td>· (Optional) For <code>port integer</code>, specify a server port number. The default is port 49. The range is 1 to 65535.</td>
<td></td>
</tr>
<tr>
<td>· (Optional) For <code>timeout integer</code>, specify a time in seconds the switch waits for a response from the daemon before it times out and declares an error. The default is 5 seconds. The range is 1 to 1000 seconds.</td>
<td></td>
</tr>
<tr>
<td>· (Optional) For <code>key string</code>, specify the encryption key for encrypting and decrypting all traffic between the switch and the TACACS+ daemon. You must configure the same key on the TACACS+ daemon for encryption to be successful.</td>
<td></td>
</tr>
<tr>
<td><code>aaa new-model</code></td>
<td>Enable AAA.</td>
</tr>
<tr>
<td><code>aaa group server tacacs+ group-name</code></td>
<td>(Optional) Define the AAA server-group with a group name.</td>
</tr>
<tr>
<td><code>server ip-address</code></td>
<td>(Optional) Associate a particular TACACS+ server with the defined server group. Repeat this step for each TACACS+ server in the AAA server group. Each server in the group must be previously defined in Step 2.</td>
</tr>
<tr>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><code>show tacacs</code></td>
<td>Verify your entries.</td>
</tr>
<tr>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To remove the specified TACACS+ server name or address, use the `no tacacs-server host hostname` global configuration command. To remove a server group from the configuration list, use the `no aaa group server tacacs+ group-name` global configuration command. To remove the IP address of a TACACS+ server, use the `no server ip-address` server group subconfiguration command.
authentication method or until all defined methods are exhausted. If authentication fails at any point in this cycle—meaning that the security server or local username database responds by denying the user access—the authentication process stops, and no other authentication methods are attempted.

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>aaa new-model Enable AAA.</td>
</tr>
</tbody>
</table>
| Step 3  | aaa authentication login {default | list-name} method1 [method2...] Create a login authentication method list.  
- To create a default list that is used when a named list is not specified in the login authentication command, use the default keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all ports.  
- For list-name, specify a character string to name the list you are creating.  
- For method1..., specify the actual method the authentication algorithm tries. The additional methods of authentication are used only if the previous method returns an error, not if it fails. |
| Step 4  | line [console | tty | vty] line-number [ending-line-number] Enter line configuration mode, and configure the lines to which you want to apply the authentication list. |
| Step 5  | login authentication {default | list-name} Apply the authentication list to a line or set of lines.  
- If you specify default, use the default list created with the aaa authentication login command.  
- For list-name, specify the list created with the aaa authentication login command. |
Chapter 7 Configuring Switch-Based Authentication

Controlling Switch Access with TACACS+

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

Configuring TACACS+ Authorization for Privileged EXEC Access and Network Services

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

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

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

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

Note

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

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>aaa authorization network tacacs+</td>
</tr>
<tr>
<td>Step 3</td>
<td>aaa authorization exec tacacs+</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
</tr>
<tr>
<td>Step 5</td>
<td>show running-config</td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To disable authorization, use the no aaa authorization {network | exec} method1 global configuration command.
Starting TACACS+ Accounting

The AAA accounting feature tracks the services that users are accessing and the amount of network resources that they are consuming. When AAA accounting is enabled, the switch reports user activity to the TACACS+ security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server. This data can then be analyzed for network management, client billing, or auditing.

Beginning in privileged EXEC mode, follow these steps to enable TACACS+ accounting for each Cisco IOS privilege level and for network services:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td><code>aaa accounting network start-stop tacacs+</code></td>
<td>Enable TACACS+ accounting for all network-related service requests.</td>
</tr>
<tr>
<td>3</td>
<td><code>aaa accounting exec start-stop tacacs+</code></td>
<td>Enable TACACS+ accounting to send a start-record accounting notice at the beginning of a privileged EXEC process and a stop-record at the end.</td>
</tr>
<tr>
<td>4</td>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>5</td>
<td><code>show running-config</code></td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>6</td>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable accounting, use the `no aaa accounting {network | exec} {start-stop} method1...` global configuration command.

Displaying the TACACS+ Configuration

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

Controlling Switch Access with RADIUS

This section describes how to enable and configure the RADIUS, which provides detailed accounting information and flexible administrative control over authentication and authorization processes. RADIUS is facilitated through AAA and can be enabled only through AAA commands.

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

This section contains this configuration information:

- Understanding RADIUS, page 7-17
- RADIUS Operation, page 7-18
- Configuring RADIUS, page 7-19
- Displaying the RADIUS Configuration, page 7-30
Understanding RADIUS

RADIUS is a distributed client/server system that secures networks against unauthorized access. RADIUS clients run on supported Cisco routers and switches. Clients send authentication requests to a central RADIUS server, which contains all user authentication and network service access information. The RADIUS host is normally a multiuser system running RADIUS server software from Cisco (Cisco Secure Access Control Server Version 3.0), Livingston, Merit, Microsoft, or another software provider. For more information, see the RADIUS server documentation.

Use RADIUS in these network environments that require access security:

- Networks with multiple-vendor access servers, each supporting RADIUS. For example, access servers from several vendors use a single RADIUS server-based security database. In an IP-based network with multiple vendors’ access servers, dial-in users are authenticated through a RADIUS server that has been customized to work with the Kerberos security system.

- Turnkey network security environments in which applications support the RADIUS protocol, such as in an access environment that uses a smart card access control system. In one case, RADIUS has been used with Enigma’s security cards to validates users and to grant access to network resources.

- Networks already using RADIUS. You can add a Cisco switch containing a RADIUS client to the network. This might be the first step when you make a transition to a TACACS+ server. See Figure 7-2 on page 7-18.

- Network in which the user must only access a single service. Using RADIUS, you can control user access to a single host, to a single utility such as Telnet, or to the network through a protocol such as IEEE 802.1x. For more information about this protocol, see Chapter 8, “Configuring IEEE 802.1x Port-Based Authentication.”

- Networks that require resource accounting. You can use RADIUS accounting independently of RADIUS authentication or authorization. The RADIUS accounting functions allow data to be sent at the start and end of services, showing the amount of resources (such as time, packets, bytes, and so forth) used during the session. An Internet service provider might use a freeware-based version of RADIUS access control and accounting software to meet special security and billing needs.

RADIUS is not suitable in these network security situations:

- Multiprotocol access environments. RADIUS does not support AppleTalk Remote Access (ARA), NetBIOS Frame Control Protocol (NBFCP), NetWare Asynchronous Services Interface (NASI), or X.25 PAD connections.

- Switch-to-switch or router-to-router situations. RADIUS does not provide two-way authentication. RADIUS can be used to authenticate from one device to a non-Cisco device if the non-Cisco device requires authentication.

- Networks using a variety of services. RADIUS generally binds a user to one service model.
RADIUS Operation

When a user attempts to log in and authenticate to a switch that is access controlled by a RADIUS server, these events occur:

1. The user is prompted to enter a username and password.
2. The username and encrypted password are sent over the network to the RADIUS server.
3. The user receives one of these responses from the RADIUS server:
   a. ACCEPT—The user is authenticated.
   b. REJECT—The user is either not authenticated and is prompted to re-enter the username and password, or access is denied.
   c. CHALLENGE—A challenge requires additional data from the user.
   d. CHALLENGE PASSWORD—A response requests the user to select a new password.

The ACCEPT or REJECT response is bundled with additional data that is used for privileged EXEC or network authorization. Users must first successfully complete RADIUS authentication before proceeding to RADIUS authorization, if it is enabled. The additional data included with the ACCEPT or REJECT packets includes these items:

- Telnet, SSH, rlogin, or privileged EXEC services
- Connection parameters, including the host or client IP address, access list, and user timeouts
Configuring RADIUS

This section describes how to configure your switch to support RADIUS. At a minimum, you must identify the host or hosts that run the RADIUS server software and define the method lists for RADIUS authentication. You can optionally define method lists for RADIUS authorization and accounting.

A method list defines the sequence and methods to be used to authenticate, to authorize, or to keep accounts on a user. You can use method lists to designate one or more security protocols to be used (such as TACACS+ or local username lookup), thus ensuring a backup system if the initial method fails. The software uses the first method listed to authenticate, to authorize, or to keep accounts on users; if that method does not respond, the software selects the next method in the list. This process continues until there is successful communication with a listed method or the method list is exhausted.

You should have access to and should configure a RADIUS server before configuring RADIUS features on your switch.

This section contains this configuration information:

- Default RADIUS Configuration, page 7-19
- Identifying the RADIUS Server Host, page 7-19 (required)
- Configuring RADIUS Login Authentication, page 7-22 (required)
- Defining AAA Server Groups, page 7-24 (optional)
- Configuring RADIUS Authorization for User Privileged Access and Network Services, page 7-26 (optional)
- Starting RADIUS Accounting, page 7-27 (optional)
- Configuring Settings for All RADIUS Servers, page 7-28 (optional)
- Configuring the Switch to Use Vendor-Specific RADIUS Attributes, page 7-28 (optional)
- Configuring the Switch for Vendor-Proprietary RADIUS Server Communication, page 7-29 (optional)
- Configuring RADIUS Server Load Balancing, page 7-30 (optional)

Default RADIUS Configuration

RADIUS and AAA are disabled by default.

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

Identifying the RADIUS Server Host

Switch-to-RADIUS-server communication involves several components:

- Hostname or IP address
- Authentication destination port
- Accounting destination port
- Key string
- Timeout period
- Retransmission value
You identify RADIUS security servers by their hostname or IP address, hostname and specific UDP port numbers, or their IP address and specific UDP port numbers. The combination of the IP address and the UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. This unique identifier enables RADIUS requests to be sent to multiple UDP ports on a server at the same IP address.

If two different host entries on the same RADIUS server are configured for the same service—for example, accounting—the second host entry configured acts as a fail-over backup to the first one. Using this example, if the first host entry fails to provide accounting services, the switch tries the second host entry configured on the same device for accounting services. (The RADIUS host entries are tried in the order that they are configured.)

A RADIUS server and the switch use a shared secret text string to encrypt passwords and exchange responses. To configure RADIUS to use the AAA security commands, you must specify the host running the RADIUS server daemon and a secret text (key) string that it shares with the switch.

The timeout, retransmission, and encryption key values can be configured globally for all RADIUS servers, on a per-server basis, or in some combination of global and per-server settings. To apply these settings globally to all RADIUS servers communicating with the switch, use the three unique global configuration commands: `radius-server timeout`, `radius-server retransmit`, and `radius-server key`. To apply these values on a specific RADIUS server, use the `radius-server host` global configuration command.

---

**Note**

If you configure both global and per-server functions (timeout, retransmission, and key commands) on the switch, the per-server timer, retransmission, and key value commands override global timer, retransmission, and key value commands. For information on configuring these setting on all RADIUS servers, see the “Configuring Settings for All RADIUS Servers” section on page 7-28.

You can configure the switch to use AAA server groups to group existing server hosts for authentication. For more information, see the “Defining AAA Server Groups” section on page 7-24.
Beginning in privileged EXEC mode, follow these steps to configure per-server RADIUS server communication. This procedure is required.

### Command Purpose

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
</tbody>
</table>
| Step 2 | radius-server host [hostname | ip-address] [auth-port port-number] [acct-port port-number] [timeout seconds] [retransmit retries] [key string] | Specify the IP address or hostname of the remote RADIUS server host.  
- (Optional) For auth-port port-number, specify the UDP destination port for authentication requests.  
- (Optional) For acct-port port-number, specify the UDP destination port for accounting requests.  
- (Optional) For timeout seconds, specify the time interval that the switch waits for the RADIUS server to reply before resending. The range is 1 to 1000. This setting overrides the radius-server timeout global configuration command setting. If no timeout is set with the radius-server host command, the setting of the radius-server timeout command is used.  
- (Optional) For retransmit retries, specify the number of times a RADIUS request is resent to a server if that server is not responding or responding slowly. The range is 1 to 1000. If no retransmit value is set with the radius-server host command, the setting of the radius-server retransmit global configuration command is used.  
- (Optional) For key string, specify the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server.  
  **Note** The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the radius-server host command. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key. |
| Step 3 | end                                           | Return to privileged EXEC mode.                          |
| Step 4 | show running-config                          | Verify your entries.                                    |
| Step 5 | copy running-config startup-config           | (Optional) Save your entries in the configuration file.  |

To remove the specified RADIUS server, use the **no radius-server host hostname | ip-address** global configuration command.

This example shows how to configure one RADIUS server to be used for authentication and another to be used for accounting:

```
Switch(config)# radius-server host 172.29.36.49 auth-port 1612 key rad1
Switch(config)# radius-server host 172.20.36.50 acct-port 1618 key rad2
```
This example shows how to configure host1 as the RADIUS server and to use the default ports for both authentication and accounting:

Switch(config)# radius-server host host1

**Note**

You also need to configure some settings on the RADIUS server. These settings include the IP address of the switch and the key string to be shared by both the server and the switch. For more information, see the RADIUS server documentation.

### Configuring RADIUS Login Authentication

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

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

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td></td>
</tr>
<tr>
<td>aaa new-model</td>
<td>Enable AAA.</td>
</tr>
</tbody>
</table>
### Controlling Switch Access with RADIUS

#### Chapter 7      Configuring Switch-Based Authentication

**Step 3**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`aaa authentication login {default</td>
<td>list-name} method1 [method2...]`</td>
</tr>
<tr>
<td></td>
<td>- To create a default list that is used when a named list is <em>not</em> specified in the <code>login authentication</code> command, use the <code>default</code> keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all ports.</td>
</tr>
<tr>
<td></td>
<td>- For <code>list-name</code>, specify a character string to name the list you are creating.</td>
</tr>
<tr>
<td></td>
<td>- For <code>method1...</code>, specify the actual method the authentication algorithm tries. The additional methods of authentication are used only if the previous method returns an error, not if it fails.</td>
</tr>
</tbody>
</table>

Select one of these methods:

- **enable**—Use the enable password for authentication. Before you can use this authentication method, you must define an enable password by using the `enable password` global configuration command.

- **group radius**—Use RADIUS authentication. Before you can use this authentication method, you must configure the RADIUS server. For more information, see the “Identifying the RADIUS Server Host” section on page 7-19.

- **line**—Use the line password for authentication. Before you can use this authentication method, you must define a line password. Use the `password password` line configuration command.

- **local**—Use the local username database for authentication. You must enter username information in the database. Use the `username name password` global configuration command.

- **local-case**—Use a case-sensitive local username database for authentication. You must enter username information in the database by using the `username name password` global configuration command.

- **none**—Do not use any authentication for login.

**Step 4**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`line [console</td>
<td>tty</td>
</tr>
</tbody>
</table>

**Step 5**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`login authentication {default</td>
<td>list-name}`</td>
</tr>
<tr>
<td></td>
<td>- If you specify <code>default</code>, use the default list created with the <code>aaa authentication login</code> command.</td>
</tr>
<tr>
<td></td>
<td>- For <code>list-name</code>, specify the list created with the <code>aaa authentication login</code> command.</td>
</tr>
</tbody>
</table>

**Step 6**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

**Step 7**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show running-config</code></td>
<td>Verify your entries.</td>
</tr>
</tbody>
</table>

**Step 8**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
To disable AAA, use the `no aaa new-model` global configuration command. To disable AAA authentication, use the `no aaa authentication login {default | list-name} method1 [method2...]` global configuration command. To either disable RADIUS authentication for logins or to return to the default value, use the `no login authentication {default | list-name}` line configuration command.

**Defining AAA Server Groups**

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

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

You use the `server group server configuration command to associate a particular server with a defined group server. You can either identify the server by its IP address or identify multiple host instances or entries by using the optional `auth-port` and `acct-port` keywords.
Beginning in privileged EXEC mode, follow these steps to define the AAA server group and associate a particular RADIUS server with it:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>radius-server host [hostname</td>
<td>Specify the IP address or hostname of the remote RADIUS</td>
</tr>
<tr>
<td></td>
<td>ip-address] [auth-port</td>
<td>server host.</td>
</tr>
<tr>
<td></td>
<td>port-number] [acct-port</td>
<td></td>
</tr>
<tr>
<td></td>
<td>port-number] [timeout</td>
<td></td>
</tr>
<tr>
<td></td>
<td>seconds] [retransmit retries]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>key string]</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) For auth-port port-number, specify the UDP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>destination port for authentication requests.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) For acct-port port-number, specify the UDP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>destination port for accounting requests.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) For timeout seconds, specify the time</td>
</tr>
<tr>
<td></td>
<td></td>
<td>interval that the switch waits for the RADIUS server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>to reply before resending. The range is 1 to 1000. This</td>
</tr>
<tr>
<td></td>
<td></td>
<td>setting overrides the radius-server timeout global</td>
</tr>
<tr>
<td></td>
<td></td>
<td>configuration command setting. If no timeout is set with</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the radius-server host command, the setting of the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>radius-server timeout command is used.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) For retransmit retries, specify the number</td>
</tr>
<tr>
<td></td>
<td></td>
<td>of times a RADIUS request is resent to a server if that</td>
</tr>
<tr>
<td></td>
<td></td>
<td>server is not responding or responding slowly. The range</td>
</tr>
<tr>
<td></td>
<td></td>
<td>is 1 to 1000. If no retransmit value is set with the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>radius-server host command, the setting of the radius-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>server retransmit global configuration command is used.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) For key string, specify the authentication</td>
</tr>
<tr>
<td></td>
<td></td>
<td>and encryption key used between the switch and the RADIUS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>daemon running on the RADIUS server.</td>
</tr>
<tr>
<td></td>
<td>Note</td>
<td>The key is a text string that must match the encryption</td>
</tr>
<tr>
<td></td>
<td></td>
<td>key used on the RADIUS server. Always configure the key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>as the last item in the radius-server host command.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Leading spaces are ignored, but spaces within and at the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>end of the key are used. If you use spaces in your key,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>do not enclose the key in quotation marks unless the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>quotation marks are part of the key.</td>
</tr>
</tbody>
</table>

To configure the switch to recognize more than one host entry associated with a single IP address, enter this command as many times as necessary, making sure that each UDP port number is different. The switch software searches for hosts in the order in which you specify them. Set the timeout, retransmit, and encryption key values to use with the specific RADIUS host.

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>aaa new-model</td>
<td>Enable AAA.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>aaa group server radius</td>
<td>Define the AAA server-group with a group name.</td>
</tr>
<tr>
<td></td>
<td>group-name</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>This command puts the switch in a server group configuration mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>server ip-address</td>
<td>Associate a particular RADIUS server with the defined</td>
</tr>
<tr>
<td></td>
<td></td>
<td>server group.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Repeat this step for each RADIUS server in the AAA server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>group. Each server in the group must be previously</td>
</tr>
<tr>
<td></td>
<td></td>
<td>defined in Step 2.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 7</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show running-config</td>
<td>Verify your entries.</td>
</tr>
</tbody>
</table>
Controlling Switch Access with RADIUS

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

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

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

Configuring RADIUS Authorization for User Privileged Access and Network Services

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

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

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

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

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

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

```
Step 1
configure terminal

Step 2
aaa authorization network radius
```

Command Purpose
---
`copy running-config startup-config` (Optional) Save your entries in the configuration file.

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

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

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

Configuring RADIUS Authorization for User Privileged Access and Network Services

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

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

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

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

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

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

```
Step 1
configure terminal

Step 2
aaa authorization network radius
```

Command Purpose
---
`copy running-config startup-config` (Optional) Save your entries in the configuration file.

Enable RADIUS login authentication. See the “Configuring RADIUS Login Authentication” section on page 7-22.
Controlling Switch Access with RADIUS

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

### Starting RADIUS Accounting

The AAA accounting feature tracks the services that users are accessing and the amount of network resources that they are consuming. When AAA accounting is enabled, the switch reports user activity to the RADIUS security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server. This data can then be analyzed for network management, client billing, or auditing.

Beginning in privileged EXEC mode, follow these steps to enable RADIUS accounting for each Cisco IOS privilege level and for network services:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>aaa accounting network start-stop radius</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>aaa accounting exec start-stop radius</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>show running-config</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To disable accounting, use the **no aaa accounting { network | exec } { start-stop } method1**... global configuration command.
Configuring Settings for All RADIUS Servers

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>radius-server key string</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>radius-server retransmit retries</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>radius-server timeout seconds</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>radius-server deadtime minutes</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>show running-config</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To return to the default setting for the retransmit, timeout, and deadtime, use the no forms of these commands.

Configuring the Switch to Use Vendor-Specific RADIUS Attributes

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific information between the switch and the RADIUS server by using the vendor-specific attribute (attribute 26). Vendor-specific attributes (VSAs) allow vendors to support their own extended attributes not suitable for general use. The Cisco RADIUS implementation supports one vendor-specific option by using the format recommended in the specification. Cisco’s vendor-ID is 9, and the supported option has vendor-type 1, which is named cisco-avpair. The value is a string with this format:

`protocol : attribute sep value *`

*Protocol* is a value of the Cisco protocol attribute for a particular type of authorization. *Attribute* and *value* are an appropriate attribute-value (AV) pair defined in the Cisco TACACS+ specification, and *sep* is = for mandatory attributes and is * for optional attributes. The full set of features available for TACACS+ authorization can then be used for RADIUS.

For example, this AV pair activates Cisco’s *multiple named ip address pools* feature during IP authorization (during PPP IPCP address assignment):

`cisco-avpair= "ip:addr-pool=first"`
Chapter 7 Configuring Switch-Based Authentication

Controlling Switch Access with RADIUS

This example shows how to provide a user logging in from a switch with immediate access to privileged EXEC commands:

cisco-avpair= "shell:priv-lvl=15"

This example shows how to specify an authorized VLAN in the RADIUS server database:

cisco-avpair= "tunnel-type(#64)=VLAN(13)"
cisco-avpair= "tunnel-medium-type(#65)=802 media(6)"
cisco-avpair= "tunnel-private-group-ID(#81)=vlanid"

This example shows how to apply an input ACL in ASCII format to a port for the duration of this connection:

cisco-avpair= "ip:inacl#1=deny ip 10.10.10.10 0.0.255.255 20.20.20.20 255.255.0.0"
cisco-avpair= "ip:inacl#2=deny ip 10.10.10.10 0.0.255.255 any"
cisco-avpair= "mac:inacl#3=deny any any decnet-iv"

This example shows how to apply an output ACL in ASCII format to a port for the duration of this connection:

cisco-avpair= "ip:outacl#2=deny ip 10.10.10.10 0.0.255.255 any"

Other vendors have their own unique vendor-IDs, options, and associated VSAs. For more information about vendor-IDs and VSAs, see RFC 2138, “Remote Authentication Dial-In User Service (RADIUS).”

Beginning in privileged EXEC mode, follow these steps to configure the switch to recognize and use VSAs:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 radius-server vsa send [accounting</td>
<td>[Optional] Use the accounting keyword to limit the set of recognized vendor-specific attributes to only accounting attributes.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enable the switch to recognize and use VSAs as defined by RADIUS IETF attribute 26.</td>
</tr>
<tr>
<td></td>
<td>If you enter this command without keywords, both accounting and authentication vendor-specific attributes are used.</td>
</tr>
<tr>
<td>Step 3 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4 show running-config</td>
<td>Verify your settings.</td>
</tr>
<tr>
<td>Step 5 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

For a complete list of RADIUS attributes or more information about vendor-specific attribute 26, see the “RADIUS Attributes” appendix in the Cisco IOS Security Configuration Guide, Release 12.2.

Configuring the Switch for Vendor-Proprietary RADIUS Server Communication

Although an IETF draft standard for RADIUS specifies a method for communicating vendor-proprietary information between the switch and the RADIUS server, some vendors have extended the RADIUS attribute set in a unique way. Cisco IOS software supports a subset of vendor-proprietary RADIUS attributes.
As mentioned earlier, to configure RADIUS (whether vendor-proprietary or IETF draft-compliant), you must specify the host running the RADIUS server daemon and the secret text string it shares with the switch. You specify the RADIUS host and secret text string by using the `radius-server` global configuration commands.

Beginning in privileged EXEC mode, follow these steps to specify a vendor-proprietary RADIUS server host and a shared secret text string:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 <code>radius-server host</code></td>
<td>Specify the IP address or hostname of the remote RADIUS server host and identify that it is using a vendor-proprietary implementation of RADIUS.</td>
</tr>
<tr>
<td>Step 3 <code>radius-server key</code></td>
<td>Specify the shared secret text string used between the switch and the vendor-proprietary RADIUS server. The switch and the RADIUS server use this text string to encrypt passwords and exchange responses.</td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5 show running-config</td>
<td>Verify your settings.</td>
</tr>
<tr>
<td>Step 6 copy running-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To delete the vendor-proprietary RADIUS host, use the `no radius-server host` global configuration command. To disable the key, use the `no radius-server key` global configuration command.

This example shows how to specify a vendor-proprietary RADIUS host and to use a secret key of `rad124` between the switch and the server:

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

**Configuring RADIUS Server Load Balancing**

This feature allows access and authentication requests to be evenly across all RADIUS servers in a server group. For more information, see the “RADIUS Server Load Balancing” chapter of the “Cisco IOS Security Configuration Guide”, Release 12.2:


**Displaying the RADIUS Configuration**

To display the RADIUS configuration, use the `show running-config` privileged EXEC command.
Controlling Switch Access with Kerberos

This section describes how to enable and configure the Kerberos security system, which authenticates requests for network resources by using a trusted third party. To use this feature, the cryptographic (that is, supports encryption) version of the switch software must be installed on your switch. You must obtain authorization to use this feature and to download the cryptographic software files from Cisco.com. For more information, see the release notes for this release.

This section consists of these topics:

- Understanding Kerberos, page 7-31
- Kerberos Operation, page 7-33
- Configuring Kerberos, page 7-34

For Kerberos configuration examples, see the “Kerberos Configuration Examples” section in the “Security Server Protocols” chapter of the Cisco IOS Security Configuration Guide, Release 12.2, at this URL:


For complete syntax and usage information for the commands used in this section, see the “Kerberos Commands” section in the “Security Server Protocols” chapter of the Cisco IOS Security Command Reference, Release 12.2, at this URL:


Note

In the Kerberos configuration examples and in the Cisco IOS Security Command Reference, Release 12.2, the trusted third party can be a Catalyst 3750 Metro switch that supports Kerberos, that is configured as a network security server, and that can authenticate users by using the Kerberos Protocol.

Understanding Kerberos

Kerberos is a secret-key network authentication protocol, which was developed at the Massachusetts Institute of Technology (MIT). It uses the Data Encryption Standard (DES) cryptographic algorithm for encryption and authentication and authenticates requests for network resources. Kerberos uses the concept of a trusted third party to perform secure verification of users and services. This trusted third party is called the key distribution center (KDC).

Kerberos verifies that users are who they claim to be and the network services that they use are what the services claim to be. To do this, a KDC or trusted Kerberos server issues tickets to users. These tickets, which have a limited lifespan, are stored in user credential caches. The Kerberos server uses the tickets instead of usernames and passwords to authenticate users and network services.

Note

A Kerberos server can be a Catalyst 3750 Metro switch that is configured as a network security server and that can authenticate users by using the Kerberos Protocol.

The Kerberos credential scheme uses a process called single logon. This process authenticates a user once and then allows secure authentication (without encrypting another password) wherever that user credential is accepted.

This software release supports Kerberos 5, which allows organizations that are already using Kerberos 5 to use the same Kerberos authentication database on the KDC that they are already using on their other network hosts (such as UNIX servers and PCs).
In this software release, Kerberos supports these network services:

- Telnet
- rlogin
- rsh (Remote Shell Protocol)

Table 7-2 lists the common Kerberos-related terms and definitions:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>A process by which a user or service identifies itself to another service. For example, a client can authenticate to a switch or a switch can authenticate to another switch.</td>
</tr>
<tr>
<td>Authorization</td>
<td>A means by which the switch identifies what privileges the user has in a network or on the switch and what actions the user can perform.</td>
</tr>
<tr>
<td>Credential</td>
<td>A general term that refers to authentication tickets, such as ticket granting tickets (TGTs) and service credentials. Kerberos credentials verify the identity of a user or service. If a network service decides to trust the Kerberos server that issued a ticket, it can be used in place of re-entering a username and password. Credentials have a default lifespan of 8 hours.</td>
</tr>
<tr>
<td>Instance</td>
<td>An authorization level label for Kerberos principals. Most Kerberos principals are of the form user@REALM (for example, <a href="mailto:smith@EXAMPLE.COM">smith@EXAMPLE.COM</a>). A Kerberos principal with a Kerberos instance has the form user/instance@REALM (for example, smith/admin@EXAMPLE.COM). The Kerberos instance can be used to specify the authorization level for the user if authentication is successful. The server of each network service might implement and enforce the authorization mappings of Kerberos instances but is not required to do so. <strong>Note</strong> The Kerberos principal and instance names must be in all lowercase characters. The Kerberos realm name must be in all uppercase characters.</td>
</tr>
<tr>
<td>KDC</td>
<td>Key distribution center (KDC) that consists of a Kerberos server and database program that is running on a network host.</td>
</tr>
<tr>
<td>Kerberized</td>
<td>A term that describes applications and services that have been modified to support the Kerberos credential infrastructure.</td>
</tr>
<tr>
<td>Kerberos realm</td>
<td>A domain consisting of users, hosts, and network services that are registered to a Kerberos server. The Kerberos server is trusted to verify the identity of a user or network service to another user or network service. <strong>Note</strong> The Kerberos realm name must be in all uppercase characters.</td>
</tr>
<tr>
<td>Kerberos server</td>
<td>A daemon that is running on a network host. Users and network services register their identity with the Kerberos server. Network services query the Kerberos server to authenticate to other network services.</td>
</tr>
<tr>
<td>KEYTAB</td>
<td>A password that a network service shares with the KDC. In Kerberos 5 and later Kerberos versions, the network service authenticates an encrypted service credential by using the key table (KEYTAB) to decrypt it. In Kerberos versions earlier than Kerberos 5, KEYTAB is referred to as server table (SRVTAB).</td>
</tr>
<tr>
<td>Principal</td>
<td>Also known as a Kerberos identity, this is who you are or what a service is according to the Kerberos server. <strong>Note</strong> The Kerberos principal name must be in all lowercase characters.</td>
</tr>
</tbody>
</table>
Kerberos Operation

A Kerberos server can be a Catalyst 3750 Metro switch that is configured as a network security server and that can authenticate remote users by using the Kerberos Protocol. Although you can customize Kerberos in a number of ways, remote users attempting to access network services must pass through three layers of security before they can access network services.

To authenticate to network services by using a Catalyst 3750 Metro switch as a Kerberos server, remote users must follow these steps:

1. **Authenticating to a Boundary Switch**, page 7-33
2. **Obtaining a TGT from a KDC**, page 7-34
3. **Authenticating to Network Services**, page 7-34

**Table 7-2 Kerberos Terms (continued)**

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service credential</td>
<td>A credential for a network service. When issued from the KDC, this credential is encrypted with the password shared by the network service and the KDC. The password is also shared with the user TGT.</td>
</tr>
<tr>
<td>SRVTAB</td>
<td>A password that a network service shares with the KDC. In Kerberos 5 or later Kerberos versions, SRVTAB is referred to as KEYTAB.</td>
</tr>
<tr>
<td>TGT</td>
<td>Ticket granting ticket that is a credential that the KDC issues to authenticated users. When users receive a TGT, they can authenticate to network services within the Kerberos realm represented by the KDC.</td>
</tr>
</tbody>
</table>

**Authenticating to a Boundary Switch**

This section describes the first layer of security through which a remote user must pass. The user must first authenticate to the boundary switch. This process then occurs:

1. The user opens an un-Kerberized Telnet connection to the boundary switch.
2. The switch prompts the user for a username and password.
3. The switch requests a TGT from the KDC for this user.
4. The KDC sends an encrypted TGT that includes the user identity to the switch.
5. The switch attempts to decrypt the TGT by using the password that the user entered.
   - If the decryption is successful, the user is authenticated to the switch.
   - If the decryption is not successful, the user repeats Step 2 either by re-entering the username and password (noting if Caps Lock or Num Lock is on or off) or by entering a different username and password.

A remote user who initiates a un-Kerberized Telnet session and authenticates to a boundary switch is inside the firewall, but the user must still authenticate directly to the KDC before getting access to the network services. The user must authenticate to the KDC because the TGT that the KDC issues is stored on the switch and cannot be used for additional authentication until the user logs on to the switch.
Controlling Switch Access with Kerberos

Obtaining a TGT from a KDC

This section describes the second layer of security through which a remote user must pass. The user must now authenticate to a KDC and obtain a TGT from the KDC to access network services.

For instructions about how to authenticate to a KDC, see the “Obtaining a TGT from a KDC” section in the “Configuring Kerberos” chapter of the “Security Server Protocols” section of the Cisco IOS Security Configuration Guide, Release 12.2, at this URL:


Authenticating to Network Services

This section describes the third layer of security through which a remote user must pass. The user with a TGT must now authenticate to the network services in a Kerberos realm.

For instructions about how to authenticate to a network service, see the “Authenticating to Network Services” section in the “Configuring Kerberos” chapter of the “Security Server Protocols” section of the Cisco IOS Security Configuration Guide, Release 12.2, at this URL:


Configuring Kerberos

So that remote users can authenticate to network services, you must configure the hosts and the KDC in the Kerberos realm to communicate and mutually authenticate users and network services. To do this, you must identify them to each other. You add entries for the hosts to the Kerberos database on the KDC and add KEYTAB files generated by the KDC to all hosts in the Kerberos realm. You also create entries for the users in the KDC database.

When you add or create entries for the hosts and users, follow these guidelines:

- The Kerberos principal name must be in all lowercase characters.
- The Kerberos instance name must be in all lowercase characters.
- The Kerberos realm name must be in all uppercase characters.

Note

A Kerberos server can be a Catalyst 3750 Metro switch that is configured as a network security server and that can authenticate users by using the Kerberos Protocol.

To set up a Kerberos-authenticated server-client system, follow these steps:

- Configure the KDC by using Kerberos commands.
- Configure the switch to use the Kerberos protocol.

For instructions, see the “Kerberos Configuration Task List” section in the “Configuring Kerberos” chapter of the “Security Server Protocols” section of the Cisco IOS Security Configuration Guide, Release 12.2, at this URL:

## Configuring the Switch for Local Authentication and Authorization

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

Beginning in privileged EXEC mode, follow these steps to configure the switch for local AAA:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> aaa new-model</td>
<td>Enable AAA.</td>
</tr>
<tr>
<td><strong>Step 3</strong> aaa authentication login default local</td>
<td>Set the login authentication to use the local username database. The default keyword applies the local user database authentication to all ports.</td>
</tr>
<tr>
<td><strong>Step 4</strong> aaa authorization exec local</td>
<td>Configure user AAA authorization, check the local database, and allow the user to run an EXEC shell.</td>
</tr>
<tr>
<td><strong>Step 5</strong> aaa authorization network local</td>
<td>Configure user AAA authorization for all network-related service requests.</td>
</tr>
<tr>
<td><strong>Step 6</strong> username name [privilege level] {password encryption-type password}</td>
<td>Enter the local database, and establish a username-based authentication system. Repeat this command for each user.</td>
</tr>
<tr>
<td></td>
<td>• For name, specify the user ID as one word. Spaces and quotation marks are not allowed.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) For level, specify the privilege level the user has after gaining access. The range is 0 to 15. Level 15 gives privileged EXEC mode access. Level 0 gives user EXEC mode access.</td>
</tr>
<tr>
<td></td>
<td>• For encryption-type, enter 0 to specify that an unencrypted password follows. Enter 7 to specify that a hidden password follows.</td>
</tr>
<tr>
<td></td>
<td>• For password, specify the password the user must enter to gain access to the switch. The password must be from 1 to 25 characters, can contain embedded spaces, and must be the last option specified in the username command.</td>
</tr>
<tr>
<td><strong>Step 7</strong> end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 8</strong> show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td><strong>Step 9</strong> copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable AAA, use the `no aaa new-model` global configuration command. To disable authorization, use the `no aaa authorization [network | exec] method` global configuration command.
To secure the switch for HTTP access by using AAA methods, you must configure the switch with the `ip http authentication aaa` global configuration command. Configuring AAA authentication does not secure the switch for HTTP access by using AAA methods.

For more information about the `ip http authentication` command, see the *Cisco IOS Security Command Reference, Release 12.2*.

### Configuring the Switch for Secure Shell

This section describes how to configure the Secure Shell (SSH) feature. To use this feature, the cryptographic (encrypted) software image must be installed on your switch. You must obtain authorization to use this feature and to download the cryptographic software files from Cisco.com. For more information, see the release notes for this release.

This section contains this information:

- **Understanding SSH**, page 7-36
- **Configuring SSH**, page 7-37
- **Displaying the SSH Configuration and Status**, page 7-40

For SSH configuration examples, see the “SSH Configuration Examples” section in the “Configuring Secure Shell” section of the “Other Security Features” section of the *Cisco IOS Security Configuration Guide, Cisco IOS Release 12.2*, at this URL:


**Note**

For complete syntax and usage information for the commands used in this section, see the command reference for this release and the command reference for Cisco IOS Release 12.2 at this URL:


### Understanding SSH

SSH is a protocol that provides a secure, remote connection to a device. SSH provides more security for remote connections than Telnet does by providing strong encryption when a device is authenticated. This software release supports SSH Version 1 (SSHv1) and SSH Version 2 (SSHv2).

This section consists of these topics:

- **SSH Servers, Integrated Clients, and Supported Versions**, page 7-36
- **Limitations**, page 7-37

### SSH Servers, Integrated Clients, and Supported Versions

The SSH feature has an SSH server and an SSH integrated client, which are applications that run on the switch. You can use an SSH client to connect to a switch running the SSH server. The SSH server works with the SSH client supported in this release and with non-Cisco SSH clients. The SSH client also works with the SSH server supported in this release and with non-Cisco SSH servers.

The switch supports an SSHv1 or an SSHv2 server.
The switch supports an SSHv1 client.  

SSH supports the Data Encryption Standard (DES) encryption algorithm, the Triple DES (3DES) encryption algorithm, and password-based user authentication. 

SSH also supports these user authentication methods:

- TACACS+ (for more information, see the “Controlling Switch Access with TACACS+” section on page 7-9)
- RADIUS (for more information, see the “Controlling Switch Access with RADIUS” section on page 7-16)
- Local authentication and authorization (for more information, see the “Configuring the Switch for Local Authentication and Authorization” section on page 7-35)

**Note**

This software release does not support IP Security (IPSec).

**Limitations**

These limitations apply to SSH:

- The switch supports Rivest, Shamir, and Adelman (RSA) authentication.
- SSH supports only the execution-shell application.
- The SSH server and the SSH client are supported only on DES (56-bit) and 3DES (168-bit) data encryption software.
- The switch supports the Advanced Encryption Standard (AES) encryption algorithm with a 128-bit key, 192-bit key, or 256-bit key. However, symmetric cipher AES to encrypt the keys is not supported.

**Configuring SSH**

This section has this configuration information:

- Configuration Guidelines, page 7-37
- Setting Up the Switch to Run SSH, page 7-38 (required)
- Configuring the SSH Server, page 7-39 (required only if you are configuring the switch as an SSH server)

**Configuration Guidelines**

Follow these guidelines when configuring the switch as an SSH server or SSH client:

- An RSA key pair generated by a SSHv1 server can be used by an SSHv2 server, and the reverse.
- If you get CLI error messages after entering the `crypto key generate rsa` global configuration command, an RSA key pair has not been generated. Reconfigure the hostname and domain, and then enter the `crypto key generate rsa` command. For more information, see the “Setting Up the Switch to Run SSH” section on page 7-38.
- When generating the RSA key pair, the message `No host name specified` might appear. If it does, you must configure a hostname by using the `hostname` global configuration command.
When generating the RSA key pair, the message *No domain specified* might appear. If it does, you must configure an IP domain name by using the `ip domain-name` global configuration command.

When configuring the local authentication and authorization authentication method, make sure that AAA is disabled on the console.

### Setting Up the Switch to Run SSH

Follow these steps to set up your switch to run SSH:

1. Download the cryptographic software image from Cisco.com. This step is required. For more information, see the release notes for this release.
2. Configure a hostname and IP domain name for the switch. Follow this procedure only if you are configuring the switch as an SSH server.
3. Generate an RSA key pair for the switch, which automatically enables SSH. Follow this procedure only if you are configuring the switch as an SSH server.
4. Configure user authentication for local or remote access. This step is required. For more information, see the “Configuring the Switch for Local Authentication and Authorization” section on page 7-35.

Beginning in privileged EXEC mode, follow these steps to configure a hostname and an IP domain name and to generate an RSA key pair. This procedure is required if you are configuring the switch as an SSH server.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>hostname hostname</td>
<td>Configure a hostname for your switch.</td>
</tr>
<tr>
<td>3</td>
<td>ip domain-name domain_name</td>
<td>Configure a host domain for your switch.</td>
</tr>
<tr>
<td>4</td>
<td>crypto key generate rsa</td>
<td>Enable the SSH server for local and remote authentication on the switch and generate an RSA key pair.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>We recommend that a minimum modulus size of 1024 bits.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>When you generate RSA keys, you are prompted to enter a modulus length. A longer modulus length might be more secure, but it takes longer to generate and to use.</td>
</tr>
<tr>
<td>5</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>6</td>
<td>show ip ssh</td>
<td>Show the version and configuration information for your SSH server.</td>
</tr>
<tr>
<td></td>
<td>or</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>show ssh</td>
<td>Show the status of the SSH server on the switch.</td>
</tr>
<tr>
<td>8</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To delete the RSA key pair, use the `crypto key zeroize rsa` global configuration command. After the RSA key pair is deleted, the SSH server is automatically disabled.
Configuring the SSH Server

Beginning in privileged EXEC mode, follow these steps to configure the SSH server:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>**ip ssh version [1</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>If you do not enter this command or do not specify a keyword, the SSH server selects the latest SSH version supported by the SSH client. For example, if the SSH client supports SSHv1 and SSHv2, the SSH server selects SSHv2.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>**ip ssh [timeout seconds</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Repeat this step when configuring both parameters.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>line vty line_number [ending_line_number]</strong> transport input ssh</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>end</strong></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>show ip ssh</strong> or <strong>show ssh</strong></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>copy running-config startup-config</strong></td>
</tr>
</tbody>
</table>

To return to the default SSH control parameters, use the **no ip ssh [timeout | authentication-retries]** global configuration command.
Displaying the SSH Configuration and Status

To display the SSH server configuration and status, use one or more of the privileged EXEC commands in Table 7-3:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip ssh</code></td>
<td>Shows the version and configuration information for the SSH server.</td>
</tr>
<tr>
<td><code>show ssh</code></td>
<td>Shows the status of the SSH server.</td>
</tr>
</tbody>
</table>

For more information about these commands, see the “Secure Shell Commands” section in the “Other Security Features” chapter of the Cisco IOS Security Command Reference, Cisco IOS Release 12.2, at this URL:


Configuring the Switch for Secure Socket Layer HTTP

This section describes how to configure Secure Socket Layer (SSL) Version 3.0 support for the HTTP 1.1 server and client. SSL provides server authentication, encryption, and message integrity, as well as HTTP client authentication, to allow secure HTTP communications. To use this feature, the cryptographic (encrypted) software image must be installed on your switch. You must obtain authorization to use this feature and to download the cryptographic software files from Cisco.com. For more information about the crypto image, see the release notes for this release.

This section contains this information:

- Understanding Secure HTTP Servers and Clients, page 7-40
- Configuring Secure HTTP Servers and Clients, page 7-42
- Displaying Secure HTTP Server and Client Status, page 7-46

For complete syntax and usage information for the commands used in this section, see the Cisco IOS Security Command Reference at this URL:


Understanding Secure HTTP Servers and Clients

On a secure HTTP connection, data to and from an HTTP server is encrypted before being sent over the Internet. HTTP with SSL encryption provides a secure connection to allow such functions as configuring a switch from a Web browser. Cisco's implementation of the secure HTTP server and secure HTTP client uses an implementation of SSL Version 3.0 with application-layer encryption. HTTP over SSL is abbreviated as HTTPS; the URL of a secure connection begins with https:// instead of http://.

The primary role of the HTTP secure server (the switch) is to listen for HTTPS requests on a designated port (the default HTTPS port is 443) and pass the request to the HTTP 1.1 Web server. The HTTP 1.1 server processes requests and passes responses (pages) back to the HTTP secure server, which, in turn, responds to the original request.
The primary role of the HTTP secure client (the web browser) is to respond to Cisco IOS application requests for HTTPS User Agent services, perform HTTPS User Agent services for the application, and pass the response back to the application.

**Certificate Authority Trustpoints**

Certificate authorities (CAs) manage certificate requests and issue certificates to participating network devices. These services provide centralized security key and certificate management for the participating devices. Specific CA servers are referred to as *trustpoints*.

When a connection attempt is made, the HTTPS server provides a secure connection by issuing a certified X.509v3 certificate, obtained from a specified CA trustpoint, to the client. The client (usually a Web browser), in turn, has a public key that allows it to authenticate the certificate.

For secure HTTP connections, we highly recommend that you configure a CA trustpoint. If a CA trustpoint is not configured for the device running the HTTPS server, the server certifies itself and generates the needed RSA key pair. Because a self-certified (self-signed) certificate does not provide adequate security, the connecting client generates a notification that the certificate is self-certified, and the user has the opportunity to accept or reject the connection. This option is useful for internal network topologies (such as testing).

If you do not configure a CA trustpoint, when you enable a secure HTTP connection, either a temporary or a persistent self-signed certificate for the secure HTTP server (or client) is automatically generated.

- If the switch is not configured with a hostname and a domain name, a temporary self-signed certificate is generated. If the switch reboots, any temporary self-signed certificate is lost, and a new temporary new self-signed certificate is assigned.
- If the switch has been configured with a host and domain name, a persistent self-signed certificate is generated. This certificate remains active if you reboot the switch or if you disable the secure HTTP server so that it will be there the next time you re-enable a secure HTTP connection.

**Note**

The certificate authorities and trustpoints must be configured on each device individually. Copying them from other devices makes them invalid on the switch.

If a self-signed certificate has been generated, this information is included in the output of the `show running-config` privileged EXEC command. This is a partial sample output from that command displaying a self-signed certificate.

```
Switch# show running-config
Building configuration...
<output truncated>
crypto pki trustpoint TP-self-signed-3080755072
   enrollment selfsigned
   subject-name cn=IOS-Self-Signed-Certificate-3080755072
   revocation-check none
   rsakeypair TP-self-signed-3080755072
!
crypto ca certificate chain TP-self-signed-3080755072
   certificate self-signed 01
      3082029F 30820208 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
      59312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
      69666931 2F302D 33303830 37353530 37323126 30240609 2A864886 F70D0109
      02161743 45322D31 3535302D 31332E73 756D6D30 342D3335 3530301E 170D3993
      30333011 30303030 35395A17 0D323030 31303130 30303030 30303030 30303030
```

Catalyst 3750 Metro Switch Software Configuration Guide
You can remove this self-signed certificate by disabling the secure HTTP server and entering the `no crypto pki trustpoint TP-self-signed-30890755072` global configuration command. If you later re-enable a secure HTTP server, a new self-signed certificate is generated.

The values that follow `TP self-signed` depend on the serial number of the device.

You can use an optional command (`ip http secure-client-auth`) to allow the HTTPS server to request an X.509v3 certificate from the client. Authenticating the client provides more security than server authentication by itself.

For additional information on Certificate Authorities, see the “Configuring Certification Authority Interoperability” chapter in the *Cisco IOS Security Configuration Guide, Release 12.2*.

**CipherSuites**

A CipherSuite specifies the encryption algorithm and the digest algorithm to use on a SSL connection. When connecting to the HTTPS server, the client Web browser offers a list of supported CipherSuites, and the client and server negotiate the best encryption algorithm to use from those on the list that are supported by both. For example, Netscape Communicator 4.76 supports U.S. security with RSA Public Key Cryptography, MD2, MD5, RC2-CBC, RC4, DES-CBC, and DES-EDE3-CBC.

For the best possible encryption, you should use a client browser that supports 128-bit encryption, such as Microsoft Internet Explorer Version 5.5 (or later) or Netscape Communicator Version 4.76 (or later). The SSL_RSA_WITH_DES_CBC_SHA CipherSuite provides less security than the other CipherSuites, as it does not offer 128-bit encryption.

The more secure and more complex CipherSuites require slightly more processing time. This list defines the CipherSuites supported by the switch and ranks them from fastest to slowest in terms of router processing load (speed):

1. SSL_RSA_WITH_DES_CBC_SHA—RSA key exchange (RSA Public Key Cryptography) with DES-CBC for message encryption and SHA for message digest
2. SSL_RSA_WITH_RC4_128_MD5—RSA key exchange with RC4 128-bit encryption and MD5 for message digest
3. SSL_RSA_WITH_RC4_128_SHA—RSA key exchange with RC4 128-bit encryption and SHA for message digest
4. SSL_RSA_WITH_3DES_EDE_CBC_SHA—RSA key exchange with 3DES and DES-EDE3-CBC for message encryption and SHA for message digest

RSA (in conjunction with the specified encryption and digest algorithm combinations) is used for both key generation and authentication on SSL connections. This usage is independent of whether or not a CA trustpoint is configured.

**Configuring Secure HTTP Servers and Clients**

This section includes procedures for configuring SSL on HTTP servers and clients. These procedures are included:

- Default SSL Configuration, page 7-43
SSL Configuration Guidelines, page 7-43
Configuring a CA Trustpoint, page 7-43
Configuring the Secure HTTP Server, page 7-44
Configuring the Secure HTTP Client, page 7-46

Default SSL Configuration

The standard HTTP server is enabled.
SSL is enabled.
No CA trustpoints are configured.
No self-signed certificates are generated.

SSL Configuration Guidelines

When SSL is used in a switch cluster, the SSL session terminates at the cluster commander. Cluster member switches must run standard HTTP.

Before you configure a CA trustpoint, you should ensure that the system clock is set. If the clock is not set, the certificate is rejected due to an incorrect date.

Configuring a CA Trustpoint

For secure HTTP connections, we recommend that you configure an official CA trustpoint. A CA trustpoint is more secure than a self-signed certificate.

Beginning in privileged EXEC mode, follow these steps to configure a CA trustpoint:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>hostname hostname</td>
</tr>
<tr>
<td></td>
<td>Specify the hostname of the switch (required only if you have not</td>
</tr>
<tr>
<td></td>
<td>previously configured a hostname). The hostname is required for security</td>
</tr>
<tr>
<td></td>
<td>keys and certificates.</td>
</tr>
<tr>
<td>Step 3</td>
<td>ip domain-name domain-name</td>
</tr>
<tr>
<td></td>
<td>Specify the IP domain name of the switch (required only if you have not</td>
</tr>
<tr>
<td></td>
<td>previously configured an IP domain name). The domain name is required</td>
</tr>
<tr>
<td></td>
<td>for security keys and certificates.</td>
</tr>
<tr>
<td>Step 4</td>
<td>crypto key generate rsa</td>
</tr>
<tr>
<td></td>
<td>(Optional) Generate an RSA key pair. RSA key pairs are required before</td>
</tr>
<tr>
<td></td>
<td>you can obtain a certificate for the switch. RSA key pairs are generated</td>
</tr>
<tr>
<td></td>
<td>automatically. You can use this command to regenerate the keys, if</td>
</tr>
<tr>
<td></td>
<td>needed.</td>
</tr>
<tr>
<td>Step 5</td>
<td>crypto ca trustpoint name</td>
</tr>
<tr>
<td></td>
<td>Specify a local configuration name for the CA trustpoint and enter CA</td>
</tr>
<tr>
<td></td>
<td>trustpoint configuration mode.</td>
</tr>
<tr>
<td>Step 6</td>
<td>enrollment url url</td>
</tr>
<tr>
<td></td>
<td>Specify the URL to which the switch should send certificate requests.</td>
</tr>
<tr>
<td>Step 7</td>
<td>enrollment http-proxy host-name port-number</td>
</tr>
<tr>
<td></td>
<td>(Optional) Configure the switch to obtain certificates from the CA</td>
</tr>
<tr>
<td></td>
<td>through an HTTP proxy server.</td>
</tr>
<tr>
<td>Step 8</td>
<td>crl query url</td>
</tr>
<tr>
<td></td>
<td>Configure the switch to request a certificate revocation list (CRL) to</td>
</tr>
<tr>
<td></td>
<td>ensure that the certificate of the peer has not been revoked.</td>
</tr>
</tbody>
</table>
## Configuring the Switch for Secure Socket Layer HTTP

### Command

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 9</strong> primary</td>
<td>(Optional) Specify that the trustpoint should be used as the primary (default) trustpoint for CA requests.</td>
</tr>
<tr>
<td><strong>Step 10</strong> exit</td>
<td>Exit CA trustpoint configuration mode and return to global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 11</strong> crypto ca authentication <code>name</code></td>
<td>Authenticate the CA by getting the public key of the CA. Use the same name used in Step 5.</td>
</tr>
<tr>
<td><strong>Step 12</strong> crypto ca enroll <code>name</code></td>
<td>Obtain the certificate from the specified CA trustpoint. This command requests a signed certificate for each RSA key pair.</td>
</tr>
<tr>
<td><strong>Step 13</strong> end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 14</strong> show crypto ca trustpoints</td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td><strong>Step 15</strong> copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Use the **no crypto ca trustpoint `name`** global configuration command to delete all identity information and certificates associated with the CA.

### Configuring the Secure HTTP Server

If you are using a certificate authority for certification, you should use the previous procedure to configure the CA trustpoint on the switch before enabling the HTTP server. If you have not configured a CA trustpoint, a self-signed certificate is generated the first time that you enable the secure HTTP server. After you have configured the server, you can configure options (path, access list to apply, maximum number of connections, or timeout policy) that apply to both standard and secure HTTP servers.

Beginning in privileged EXEC mode, follow these steps to configure a secure HTTP server:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** show ip http server status | (Optional) Display the status of the HTTP server to determine if the secure HTTP server feature is supported in the software. You should see one of these lines in the output:  
HTTP secure server capability: Present  
or  
HTTP secure server capability: Not present |
| **Step 2** configure terminal     | Enter global configuration mode.                                                                                                       |
| **Step 3** ip http secure-server  | Enable the HTTPS server if it has been disabled. The HTTPS server is enabled by default.                                              |
| **Step 4** ip http secure-port `port-number` | (Optional) Specify the port number to be used for the HTTPS server. The default port number is 443. Valid options are 443 or any number in the range 1025 to 65535. |
| **Step 5** ip http secure-ciphersuite `[3des-ede-cbc-sha] [rc4-128-md5] [rc4-128-sha] [des-cbc-sha]` | (Optional) Specify the CipherSuites (encryption algorithms) to be used for encryption over the HTTPS connection. If you do not have a reason to specify a particularly CipherSuite, you should allow the server and client to negotiate a CipherSuite that they both support. This is the default. |
### Command and Purpose

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 6</td>
<td>ip http secure-client-auth</td>
<td>(Optional) Configure the HTTP server to request an X.509v3 certificate from the client for authentication during the connection process. The default is for the client to request a certificate from the server, but the server does not attempt to authenticate the client.</td>
</tr>
<tr>
<td>Step 7</td>
<td>ip http secure-trustpoint name</td>
<td>Specify the CA trustpoint to use to get an X.509v3 security certificate and to authenticate the client certificate connection.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> Use of this command assumes you have already configured a CA trustpoint according to the previous procedure.</td>
</tr>
<tr>
<td>Step 8</td>
<td>ip http path path-name</td>
<td>(Optional) Set a base HTTP path for HTML files. The path specifies the location of the HTTP server files on the local system (usually located in system flash memory).</td>
</tr>
<tr>
<td>Step 9</td>
<td>ip http access-class access-list-number</td>
<td>(Optional) Specify an access list to use to allow access to the HTTP server.</td>
</tr>
<tr>
<td>Step 10</td>
<td>ip http max-connections value</td>
<td>(Optional) Set the maximum number of concurrent connections that are allowed to the HTTP server. The range is 1 to 16; the default value is 5.</td>
</tr>
<tr>
<td>Step 11</td>
<td>ip http timeout-policy idle seconds life seconds requests value</td>
<td>(Optional) Specify how long a connection to the HTTP server can remain open under the defined circumstances:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>idle</strong>—the maximum time period when no data is received or response data cannot be sent. The range is 1 to 600 seconds. The default is 180 seconds (3 minutes).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>life</strong>—the maximum time period from the time that the connection is established. The range is 1 to 86400 seconds (24 hours). The default is 180 seconds.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>requests</strong>—the maximum number of requests processed on a persistent connection. The maximum value is 86400. The default is 1.</td>
</tr>
<tr>
<td>Step 12</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 13</td>
<td>show ip http server secure status</td>
<td>Display the status of the HTTP secure server to verify the configuration.</td>
</tr>
<tr>
<td>Step 14</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Use the `no ip http server` global configuration command to disable the standard HTTP server. Use the `no ip http secure-server` global configuration command to disable the secure HTTP server. Use the `no ip http secure-port` and the `no ip http secure-ciphersuite` global configuration commands to return to the default settings. Use the `no ip http secure-client-auth` global configuration command to remove the requirement for client authentication.

To verify the secure HTTP connection by using a Web browser, enter https://URL, where the URL is the IP address or hostname of the server switch. If you configure a port other than the default port, you must also specify the port number after the URL. For example:

```
https://209.165.129:1026
```

or

```
https://host.domain.com:1026
```
Configuring the Secure HTTP Client

The standard HTTP client and secure HTTP client are always enabled. A certificate authority is required for secure HTTP client certification. This procedure assumes that you have previously configured a CA trustpoint on the switch. If a CA trustpoint is not configured and the remote HTTPS server requires client authentication, connections to the secure HTTP client fail.

Beginning in privileged EXEC mode, follow these steps to configure a secure HTTP client:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip http client secure-trustpoint name</td>
</tr>
<tr>
<td>Step 3</td>
<td>ip http client secure-ciphersuite {(3des-ede-cbc-sha</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
</tr>
<tr>
<td>Step 5</td>
<td>show ip http client secure status</td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

Use the no ip http client secure-trustpoint name to remove a client trustpoint configuration. Use the no ip http client secure-ciphersuite to remove a previously configured CipherSuite specification for the client.

Displaying Secure HTTP Server and Client Status

To display the SSL secure server and client status, use the privileged EXEC commands in Table 7-4:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip http client secure status</td>
<td>Shows the HTTP secure client configuration.</td>
</tr>
<tr>
<td>show ip http server secure status</td>
<td>Shows the HTTP secure server configuration.</td>
</tr>
<tr>
<td>show running-config</td>
<td>Shows the generated self-signed certificate for secure HTTP connections.</td>
</tr>
</tbody>
</table>

Configuring the Switch for Secure Copy Protocol

The Secure Copy Protocol (SCP) feature provides a secure and authenticated method for copying switch configurations or switch image files. SCP relies on Secure Shell (SSH), an application and a protocol that provides a secure replacement for the Berkeley r-tools.
For SSH to work, the switch needs an RSA public/private key pair. This is the same with SCP, which relies on SSH for its secure transport.

Because SSH also relies on AAA authentication, and SCP relies further on AAA authorization, correct configuration is necessary.

- Before enabling SCP, you must correctly configure SSH, authentication, and authorization on the switch.
- Because SCP relies on SSH for its secure transport, the router must have an Rivest, Shamir, and Adelman (RSA) key pair.

**Note**

When using SCP, you cannot enter the password into the copy command. You must enter the password when prompted.

**Information About Secure Copy**

To configure the Secure Copy feature, you should understand these concepts.

- The behavior of SCP is similar to that of remote copy (rcp), which comes from the Berkeley r-tools suite, except that SCP relies on SSH for security. SCP also requires that authentication, authorization, and accounting (AAA) authorization be configured so the router can determine whether the user has the correct privilege level.
- A user who has appropriate authorization can use SCP to copy any file in the Cisco IOS File System (IFS) to and from a switch by using the `copy` command. An authorized administrator can also do this from a workstation.

For information about how to configure and verify SCP, see the "Secure Copy Protocol" section in the *Cisco IOS Security Configuration Guide: Securing User Services, Release 12.4*:  
8

CHAPTER

Configuring IEEE 802.1x Port-Based Authentication

This chapter describes how to configure IEEE 802.1x port-based authentication on the Catalyst 3750 Metro switch. As LANs extend to hotels, airports, and corporate lobbies, creating insecure environments, IEEE 802.1x prevents unauthorized devices (clients) from gaining access to the network.

For complete syntax and usage information for the commands used in this chapter, see the command reference for this release.

Note

Some IEEE 802.1x (dot1x) commands are visible on the switch but are not supported. For a list of unsupported commands see Appendix C, “Unsupported Commands in Cisco IOS Release 12.2(55)SE.”

This chapter consists of these sections:

- Understanding IEEE 802.1x Port-Based Authentication, page 8-1
- Configuring IEEE 802.1x Authentication, page 8-14
- Displaying 802.1x Statistics and Status, page 8-35

Understanding IEEE 802.1x Port-Based Authentication

The IEEE 802.1x standard defines a client-server-based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. The authentication server authenticates each client connected to a switch port before making available any services offered by the switch or the LAN.

Until the client is authenticated, IEEE 802.1x access control allows only Extensible Authentication Protocol over LAN (EAPOL), Cisco Discovery Protocol (CDP), and Spanning Tree Protocol (STP) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.

These sections describe IEEE 802.1x port-based authentication:

- Device Roles, page 8-2
- Authentication Initiation and Message Exchange, page 8-3
- Ports in Authorized and Unauthorized States, page 8-4
- 802.1x Accounting, page 8-5
- Supported Topologies, page 8-5
Device Roles

With IEEE 802.1x port-based authentication, the devices in the network have specific roles as shown in Figure 8-1.

- **Client**—the device (workstation) that requests access to the LAN and switch services and responds to requests from the switch. The workstation must be running IEEE 802.1x-compliant client software such as that offered in the Microsoft Windows XP operating system. (The client is the *supplicant* in the IEEE 802.1x specification.)

  **Note**  To resolve Windows XP network connectivity and IEEE 802.1x authentication issues, read the Microsoft Knowledge Base article at this URL:  
  [http://support.microsoft.com/support/kb/articles/Q303/5/97.ASP](http://support.microsoft.com/support/kb/articles/Q303/5/97.ASP)

- **Authentication server**—performs the actual authentication of the client. The authentication server validates the identity of the client and notifies the switch whether or not the client is authorized to access the LAN and switch services. Because the switch acts as the proxy, the authentication service is transparent to the client. In this release, the RADIUS security system with Extensible Authentication Protocol (EAP) extensions is the only supported authentication server. It is available...
in Cisco Secure Access Control Server Version 3.0 or later. RADIUS operates in a client/server model in which secure authentication information is exchanged between the RADIUS server and one or more RADIUS clients.

- **Switch** (edge switch or wireless access point)—controls the physical access to the network based on the authentication status of the client. The switch acts as an intermediary (proxy) between the client and the authentication server, requesting identity information from the client, verifying that information with the authentication server, and relaying a response to the client. The switch includes the RADIUS client, which is responsible for encapsulating and decapsulating the EAP frames and interacting with the authentication server.

When the switch receives EAPOL frames and relays them to the authentication server, the Ethernet header is stripped and the remaining EAP frame is re-encapsulated in the RADIUS format. The EAP frames are not modified or examined during encapsulation, and the authentication server must support EAP within the native frame format. When the switch receives frames from the authentication server, the server’s frame header is removed, leaving the EAP frame, which is then encapsulated for Ethernet and sent to the client.

The devices that can act as intermediaries include the Catalyst 3750, Catalyst 3550, Catalyst 2970, Catalyst 2955, Catalyst 2950, Catalyst 2940 switches, or a wireless access point. These devices must be running software that supports the RADIUS client and IEEE 802.1x.

---

**Authentication Initiation and Message Exchange**

The switch or the client can initiate authentication. If you enable authentication on a port by using the `dot1x port-control auto` interface configuration command, the switch must initiate authentication when the port link state transitions from down to up. It then sends an EAP-request/identity frame to the client to request its identity (typically, the switch sends an initial identity/request frame followed by one or more requests for authentication information). Upon receipt of the frame, the client responds with an EAP-response/identity frame.

However, if during bootup, the client does not receive an EAP-request/identity frame from the switch, the client can initiate authentication by sending an EAPOL-start frame, which prompts the switch to request the client’s identity.

---

**Note**

If IEEE 802.1x is not enabled or supported on the network access device, any EAPOL frames from the client are dropped. If the client does not receive an EAP-request/identity frame after three attempts to start authentication, the client sends frames as if the port is in the authorized state. A port in the authorized state effectively means that the client has been successfully authenticated. For more information, see the “Ports in Authorized and Unauthorized States” section on page 8-4.

When the client supplies its identity, the switch begins its role as the intermediary, passing EAP frames between the client and the authentication server until authentication succeeds or fails. If the authentication succeeds, the switch port becomes authorized. For more information, see the “Ports in Authorized and Unauthorized States” section on page 8-4.

The specific exchange of EAP frames depends on the authentication method being used. Figure 8-2 shows a message exchange initiated by the client when the client uses the One-Time-Password (OTP) authentication method with a RADIUS server.
Ports in Authorized and Unauthorized States

Depending on the switch port state, the switch can grant a client access to the network. The port starts in the unauthorized state. While in this state, the port disallows all ingress and egress traffic except for IEEE 802.1x, CDP, and STP protocol packets. When a client is successfully authenticated, the port transitions to the authorized state, allowing all traffic for the client to flow normally.

If a client that does not support IEEE 802.1x is connected to an unauthorized IEEE 802.1x port, the switch requests the client’s identity. In this situation, the client does not respond to the request, the port remains in the unauthorized state, and the client is not granted access to the network.

In contrast, when an IEEE 802.1x-enabled client connects to a port that is not running the IEEE 802.1x protocol, the client initiates the authentication process by sending the EAPOL-start frame. When no response is received, the client sends the request for a fixed number of times. Because no response is received, the client begins sending frames as if the port is in the authorized state.

You control the port authorization state by using the `dot1x port-control` interface configuration command and these keywords:

- **force-authorized**—disables IEEE 802.1x authentication and causes the port to transition to the authorized state without any authentication exchange required. The port sends and receives normal traffic without IEEE 802.1x-based authentication of the client. This is the default setting.

- **force-unauthorized**—causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the port.

- **auto**—enables IEEE 802.1x authentication and causes the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up or when an EAPOL-start frame is received. The switch requests the identity of the client and begins relaying authentication messages between the client and the authentication server. Each client attempting to access the network is uniquely identified by the switch by using the client MAC address.
If the client is successfully authenticated (receives an Accept frame from the authentication server), the port state changes to authorized, and all frames from the authenticated client are allowed through the port. If the authentication fails, the port remains in the unauthorized state, but authentication can be retried. If the authentication server cannot be reached, the switch can resend the request. If no response is received from the server after the specified number of attempts, authentication fails, and network access is not granted.

When a client logs off, it sends an EAPOL-logoff message, causing the switch port to transition to the unauthorized state.

If the link state of a port transitions from up to down, or if an EAPOL-logoff frame is received, the port returns to the unauthorized state.

**802.1x Accounting**

The IEEE 802.1x standard defines how users are authorized and authenticated for network access but does not keep track of network usage. IEEE 802.1x accounting is disabled by default. You can enable IEEE 802.1x accounting to monitor this activity on IEEE 802.1x-enabled ports:

- User successfully authenticates.
- User logs off.
- Link-down occurs.
- Re-authentication successfully occurs.
- Re-authentication fails.

The switch does not log IEEE 802.1x accounting information. Instead, it sends this information to the RADIUS server, which must be configured to log accounting messages.

**Supported Topologies**

The IEEE 802.1x port-based authentication is supported in two topologies:

- Point-to-point
- Wireless LAN

In a point-to-point configuration (see Figure 8-1 on page 8-2), only one client can be connected to the IEEE 802.1x-enabled switch port. The switch detects the client when the port link state changes to the up state. If a client leaves or is replaced with another client, the switch changes the port link state to down, and the port returns to the unauthorized state.

Figure 8-3 shows IEEE 802.1x port-based authentication in a wireless LAN. The IEEE 802.1x port is configured as a multiple-hosts port that becomes authorized as soon as one client is authenticated. When the port is authorized, all other hosts indirectly attached to the port are granted access to the network. If the port becomes unauthorized (re-authentication fails or an EAPOL-logoff message is received), the switch denies access to the network to all of the attached clients. In this topology, the wireless access point is responsible for authenticating the clients attached to it, and the wireless access point acts as a client to the switch.
Chapter 8  Configuring IEEE 802.1x Port-Based Authentication

Understanding IEEE 802.1x Port-Based Authentication

Figure 8-3 Wireless LAN Example

802.1x Readiness Check

The 802.1x readiness check monitors IEEE 802.1x activity on all the switch ports and displays information about the devices connected to the ports that support IEEE 802.1x. You can use this feature to determine if the devices connected to the switch ports are IEEE 802.1x-capable. You use an alternate authentication for the devices that do not support IEEE 802.1x functionality.

This feature only works if the supplicant on the client supports a query with the NOTIFY EAP notification packet. The client must respond within the IEEE 802.1x timeout value.

For information on configuring the switch for the 802.1x readiness check, see the “Configuring 802.1x Readiness Check” section on page 8-17.

802.1x with Port Security

You can configure IEEE 802.1x port and port security in either single-host or multiple-hosts mode. (You also must configure port security on the port by using the switchport port-security interface configuration command.) When you enable port security and IEEE 802.1x on a port, IEEE 802.1x authenticates the port, and port security manages network access for all MAC addresses, including that of the client. You can then limit the number or group of clients that can access the network through an IEEE 802.1x port.

These are some examples of the interaction between IEEE 802.1x and port security on the switch:

- When a client is authenticated, and the port security table is not full, the client MAC address is added to the port security list of secure hosts. The port then proceeds to come up normally.

- When a client is authenticated and manually configured for port security, it is guaranteed an entry in the secure host table (unless port security static aging has been enabled).

- A security violation occurs if the client is authenticated, but the port security table is full. This can happen if the maximum number of secure hosts has been statically configured or if the client ages out of the secure host table. If the client address is aged, its place in the secure host table can be taken by another host.

- If the security violation is caused by the first authenticated host, the port becomes error-disabled and immediately shuts down.

The port security violation modes determine the action for security violations. For more information, see the “Security Violations” section on page 24-10.
When you manually remove an IEEE 802.1x client address from the port security table by using the `no switchport port-security mac-address mac-address` interface configuration command, you should re-authenticate the IEEE 802.1x client by using the `dot1x re-authenticate interface interface-id` privileged EXEC command.

When an IEEE 802.1x client logs off, the port transitions to an unauthenticated state, and all dynamic entries in the secure host table are cleared, including the entry for the client. Normal authentication then takes place.

If the port is administratively shut down, the port becomes unauthenticated, and all dynamic entries are removed from the secure host table.

Port security and a voice VLAN can be configured simultaneously on an IEEE 802.1x port that is in either single-host or multiple-hosts mode. Port security applies to both the voice VLAN identifier (VVID) and the port VLAN identifier (PVID).

You can configure the `dot1x violation-mode` interface configuration command so that a port shuts down, generates a syslog error, or discards packets from a new device when it connects to an IEEE 802.1x-enabled port or when the maximum number of allowed devices have been authenticated. For more information see the “Maximum Number of Allowed Devices Per Port” section on page 8-17 and the command reference for this release.

For more information about enabling port security on your switch, see the “Configuring Port Security” section on page 24-8.

802.1x with Voice VLAN Ports

A voice VLAN port is a special access port associated with two VLAN identifiers:

- **VVID** to carry voice traffic to and from the IP phone. The VVID is used to configure the IP phone connected to the port.
- **PVID** to carry the data traffic to and from the workstation connected to the switch through the IP phone. The PVID is the native VLAN of the port.

Each port that you configure for a voice VLAN is associated with a PVID and a VVID. This configuration allows voice traffic and data traffic to be separated onto different VLANs. The IP phone uses the VVID for its voice traffic regardless of the authorized or unauthorized state of the port. This allows the phone to work independently of IEEE 802.1x authentication.

When you enable the single-host mode, multiple IP phones are allowed on the VVID; only one IEEE 802.1x client is allowed on the PVID. When you enable the multiple-hosts mode and when an IEEE 802.1x user is authenticated on the primary VLAN, additional clients on the voice VLAN are unrestricted after IEEE 802.1x authentication succeeds on the primary VLAN.

A voice VLAN port becomes active when there is link, and the device MAC address appears after the first CDP message from the IP phone. Cisco IP phones do not relay CDP messages from other devices. As a result, if several IP phones are connected in series, the switch recognizes only the one directly connected to it. When IEEE 802.1x is enabled on a voice VLAN port, the switch drops packets from unrecognized IP phones more than one hop away.

When IEEE 802.1x is enabled on a port, you cannot configure a port VLAN that is equal to a voice VLAN.

For more information about voice VLANs, see the Chapter 14, “Configuring Voice VLAN.”
802.1x with VLAN Assignment

The switch supports IEEE 802.1x with VLAN assignment. After successful IEEE 802.1x authentication of a port, the RADIUS server sends the VLAN assignment to configure the switch port. The RADIUS server database maintains the username-to-VLAN mappings, which assigns the VLAN based on the username of the client connected to the switch port. You can use this feature to limit network access for certain users.

When configured on the switch and the RADIUS server, IEEE 802.1x with VLAN assignment has these characteristics:

- If no VLAN is supplied by the RADIUS server or if IEEE 802.1x authorization is disabled, the port is configured in its access VLAN after successful authentication.
- If IEEE 802.1x authorization is enabled but the VLAN information from the RADIUS server is not valid, the port returns to the unauthorized state and remains in the configured access VLAN. This prevents ports from appearing unexpectedly in an inappropriate VLAN because of a configuration error.
- Configuration errors could include specifying a VLAN for a routed port, a malformed VLAN ID, a nonexistent or internal (routed port) VLAN ID, or an attempted assignment to a voice VLAN ID.
- If IEEE 802.1x authorization is enabled and all information from the RADIUS server is valid, the port is placed in the specified VLAN after authentication.
- If the multiple-hosts mode is enabled on an IEEE 802.1x port, all hosts are placed in the same VLAN (specified by the RADIUS server) as the first authenticated host.
- If IEEE 802.1x and port security are enabled on a port, the port is placed in RADIUS server assigned VLAN.
- If IEEE 802.1x is disabled on the port, it is returned to the configured access VLAN.

When the port is in the force authorized, force unauthorized, unauthorized, or shutdown state, it is put into the configured access VLAN.

If an IEEE 802.1x port is authenticated and put in the RADIUS server assigned VLAN, any change to the port access VLAN configuration does not take effect.

The IEEE 802.1x with VLAN assignment feature is not supported on trunk ports, dynamic ports, or with dynamic-access port assignment through a VLAN Membership Policy Server (VMPS).

To configure VLAN assignment you need to perform these tasks:

- Enable AAA authorization by using the network keyword to allow port configuration from the RADIUS server.
- Enable IEEE 802.1x. (The VLAN assignment feature is automatically enabled when you configure IEEE 802.1x on an access port).
- Assign vendor-specific tunnel attributes in the RADIUS server. The RADIUS server must return these attributes to the switch:
  - [64] Tunnel-Type = VLAN
  - [65] Tunnel-Medium-Type = 802
  - [81] Tunnel-Private-Group-ID = VLAN name or VLAN ID

Attribute [64] must contain the value VLAN (type 13). Attribute [65] must contain the value 802 (type 6). Attribute [81] specifies the VLAN name or VLAN ID assigned to the IEEE 802.1x-authenticated user.
For examples of tunnel attributes, see the “Configuring the Switch to Use Vendor-Specific RADIUS Attributes” section on page 7-28.

802.1x with Guest VLAN

You can configure a guest VLAN for each IEEE 802.1x port on the switch to provide limited services to clients (for example, how to download the IEEE 802.1x client). These clients might be upgrading their system for IEEE 802.1x authentication, and some hosts, such as Windows 98 systems, might not be IEEE 802.1x-capable.

When the authentication server does not receive a response to its EAP request/identity frame, clients that are not IEEE 802.1x-capable are put into the guest VLAN for the port, if one is configured. However, the server does not grant IEEE 802.1x-capable clients that fail authentication access to the network.

The switch maintains the EAPOL packet history. If an EAPOL packet is detected on the interface during the lifetime of the link, the switch determines that the device connected to that interface is an IEEE 802.1x-capable supplicant, and the interface does not transition to the guest VLAN state. EAPOL history is cleared if the interface link status goes down. If no EAPOL packet is detected on the interface, it is transitioned to the guest VLAN state.

If the switch is trying to authorize an IEEE 802.1x-capable voice device and the AAA server is unavailable, the authorization attempt fails, but the detection of the EAPOL packet is saved in the EAPOL history. When the AAA server becomes available, the switch authorizes the voice device. However, the switch no longer allows other devices access to the guest VLAN. To prevent this situation, use one of these command sequences:

- Enter the `dot1x guest-vlan supplicant` global configuration command to allow access to the guest VLAN.
- Enter the `shutdown` interface configuration command followed by the `no shutdown` interface configuration command to restart the port.

If an EAPOL packet is detected on the wire after the interface has transitioned to the guest VLAN, the interface reverts to an unauthorized state, and IEEE 802.1x authentication restarts.

Any number of hosts are allowed access when the switch port is moved to the guest VLAN. If an IEEE 802.1x-capable host joins the same port on which the guest VLAN is configured, the port is put into the unauthorized state in the user-configured access VLAN, and authentication is restarted.

Guest VLANs are supported on IEEE 802.1x ports in single-host or multiple-hosts mode.

You can configure any active VLAN except an RSPAN VLAN or a voice VLAN as an IEEE 802.1x guest VLAN. The guest VLAN feature is not supported on internal VLANs (routed ports) or trunk ports; it is supported only on access ports.

For more information, see the “Configuring a Guest VLAN” section on page 8-26.
802.1x with Restricted VLAN

You can configure a restricted VLAN (sometimes called an *authentication failed VLAN*) for each IEEE 802.1x port on a switch to provide limited services to clients that cannot access the guest VLAN. These clients are IEEE 802.1x-compliant and cannot access another VLAN because they fail the authentication process. A restricted VLAN allows users without valid credentials on an authentication server (typically, visitors to an enterprise) to access a limited set of services. The administrator can control the services available to the restricted VLAN.

Note

You can configure a VLAN to be both the guest VLAN and the restricted VLAN if you want to provide the same services to both types of users.

Without this feature, the client indefinitely attempts and fails authentication and the switch port remains in the spanning-tree blocking state. With this feature, you can configure the switch port to be in the restricted VLAN after a specified number of authentication attempts (the default value is 3 attempts).

The authenticator counts the failed authentication attempts for the client. When this count exceeds the configured maximum authentication attempts, the port moves to the restricted VLAN. The failed attempt count increments when the RADIUS server replies with either an *EAP failure* or an empty response without an EAP packet. When the port moves into the restricted VLAN, the failed attempt counter resets.

Users who fail authentication remain in the restricted VLAN until the next re-authentication attempt. A port in the restricted VLAN tries to re-authenticate at configured intervals (the default is 60 seconds). If re-authentication fails, the port remains in the restricted VLAN. If re-authentication is successful, the port moves either to the configured VLAN or to a VLAN sent by the RADIUS server. You can disable re-authentication. If you do this, the only way to start the authentication process again is for the port to receive a *link down* or *EAP logoff* event. We recommend that you keep re-authentication enabled if a client might connect through a hub. When a client disconnects from the hub, the port might not receive the *link down* or *EAP logoff* event.

After a port moves to the restricted VLAN, it sends a simulated EAP success message to the client instead of an EAP failure message. This prevents clients from indefinitely attempting authentication. Some clients (for example, devices running Windows XP) cannot implement DHCP without EAP success.

Restricted VLANs are supported only on IEEE 802.1x ports in single-host mode and on Layer 2 ports.

You can configure any active VLAN except an RSPAN VLAN, a primary private VLAN, or a voice VLAN as an IEEE 802.1x restricted VLAN. The restricted VLAN feature is not supported on internal VLANs (routed ports) or trunk ports; it is supported only on access ports.

This feature works with port security. As soon as the port is authorized, a MAC address is provided to port security. If port security does not permit the MAC address or if the maximum secure address count is reached, the port becomes unauthorized and error-disabled.

Other port security features such as Dynamic ARP Inspection, DHCP snooping, and IP source guard can be configured independently on a restricted VLAN.
Understanding IEEE 802.1x Port-Based Authentication

802.1x with Per-User ACLs

You can enable per-user access control lists (ACLs) to provide different levels of network access and service to an IEEE 802.1x-authenticated user. When the RADIUS server authenticates a user connected to an IEEE 802.1x port, it retrieves the ACL attributes based on the user identity and sends them to the switch. The switch applies the attributes to the IEEE 802.1x port for the duration of the user session. The switch removes the per-user ACL configuration when the session is over, if authentication fails, or if a link-down condition occurs. The switch does not save RADIUS-specified ACLs in the running configuration. When the port is unauthorized, the switch removes the ACL from the port.

You can configure router ACLs and input port ACLs. However, a port ACL takes precedence over a router ACL. If you apply input port ACL to a port that belongs to a VLAN, the port ACL takes precedence over an input router ACL applied to the VLAN interface. Incoming packets received on the port to which a port ACL is applied are filtered by the port ACL. Incoming routed packets received on other ports are filtered by the router ACL. Outgoing routed packets are filtered by the router ACL. To avoid configuration conflicts, you should carefully plan the user profiles stored on the RADIUS server.

RADIUS supports per-user attributes, including vendor-specific attributes. These vendor-specific attributes (VSAs) are in octet-string format and are passed to the switch during the authentication process. The VSAs used for per-user ACLs are \textit{in\text{\texttt{accl}\#<n>}} for the ingress direction and \textit{out\text{\texttt{accl}\#<n>}} for the egress direction. MAC ACLs are supported only in the ingress direction. The switch supports VSAs only in the ingress direction. It does not support port ACLs in the egress direction on Layer 2 ports. For more information, see Chapter 33, “Configuring Network Security with ACLs.”

Use only the extended ACL syntax style to define the per-user configuration stored on the RADIUS server. When the definitions are passed from the RADIUS server, they are created by using the extended naming convention. However, if you use the Filter-Id attribute, it can point to a standard ACL.

You can use the Filter-Id attribute to specify an inbound or outbound ACL that is already configured on the switch. The attribute contains the ACL number followed by .\textit{in} for ingress filtering or .\textit{out} for egress filtering. If the RADIUS server does not allow the .\textit{in} or .\textit{out} syntax, the access list is applied to the outbound ACL by default. Because of limited support of Cisco IOS access lists on the switch, the Filter-Id attribute is supported only for IP ACLs numbered 1 to 199 and 1300 to 2699 (IP standard and IP extended ACLs).

Only one IEEE 802.1x-authenticated user is supported on a port. If the multiple-hosts mode is enabled on the port, the per-user ACL attribute is disabled for the associated port.

The maximum size of the per-user ACL is 4000 ASCII characters.

For examples of vendor-specific attributes, see the “Configuring the Switch to Use Vendor-Specific RADIUS Attributes” section on page 7-28. For more information about configuring ACLs, see Chapter 33, “Configuring Network Security with ACLs.”

To configure per-user ACLs, you need to perform these tasks:

- Enable AAA authentication.
- Enable AAA authorization by using the \textbf{network} keyword to allow port configuration from the RADIUS server.
- Enable IEEE 802.1x.
- Configure the user profile and VSAs on the RADIUS server.
- Configure the IEEE 802.1x port for single-host mode.

\textbf{Note} Per-user ACLs are supported only in single-host mode.
802.1x User Distribution

You can configure 802.1x user distribution to load-balance users with the same group name across multiple different VLANs.

The VLANs are either supplied by the RADIUS server or configured through the switch CLI under a VLAN group name.

- Configure the RADIUS server to send more than one VLAN name for a user. The multiple VLAN names can be sent as part of the response to the user. The 802.1x user distribution tracks all the users in a particular VLAN and achieves load balancing by moving the authorized user to the least populated VLAN.

- Configure the RADIUS server to send a VLAN group name for a user. The VLAN group name can be sent as part of the response to the user. You can search for the selected VLAN group name among the VLAN group names that you configured by using the switch CLI. If the VLAN group name is found, the corresponding VLANs under this VLAN group name are searched to find the least populated VLAN. Load balancing is achieved by moving the corresponding authorized user to that VLAN.

Note: The RADIUS server can send the VLAN information in any combination of VLAN-IDs, VLAN names, or VLAN groups.

802.1x User Distribution Configuration Guidelines

- Confirm that at least one VLAN is mapped to the VLAN group.
- You can map more than one VLAN to a VLAN group.
- You can modify the VLAN group by adding or deleting a VLAN.
- When you clear an existing VLAN from the VLAN group name, none of the authenticated ports in the VLAN are cleared, but the mappings are removed from the existing VLAN group.
- If you clear the last VLAN from the VLAN group name, the VLAN group is cleared.
- You can clear a VLAN group even when the active VLANs are mapped to the group. When you clear a VLAN group, none of the ports or users that are in the authenticated state in any VLAN within the group are cleared, but the VLAN mappings to the VLAN group are cleared.

For more information, see the “Configuring 802.1x User Distribution” section on page 8-30.

802.1x Supplicant and Authenticator Switches with Network Edge Access Topology (NEAT)

The Network Edge Access Topology (NEAT) feature extends identity to areas outside the wiring closet (such as conference rooms). This allows any type of device to authenticate on the port.

- 802.1x switch supplicant: You can configure a switch to act as a supplicant to another switch by using the 802.1x supplicant feature. This configuration is helpful in a scenario, where, for example, a switch is outside a wiring closet and is connected to an upstream switch through a trunk port. A switch configured with the 802.1x switch supplicant feature authenticates with the upstream switch for secure connectivity.

Once the supplicant switch authenticates successfully the port mode changes from access to trunk.
If the access VLAN is configured on the authenticator switch, it becomes the native VLAN for the trunk port after successful authentication.

You can enable MDA or multiauth mode on the authenticator switch interface that connects to one more supplicant switches. Multihost mode is not supported on the authenticator switch interface.

Use the `dot1x supplicant force-multicast` global configuration command on the supplicant switch for Network Edge Access Topology (NEAT) to work in all host modes.

- **Host Authorization**: Ensures that only traffic from authorized hosts (connecting to the switch with supplicant) is allowed on the network. The switches use Client Information Signalling Protocol (CISP) to send the MAC addresses connecting to the supplicant switch to the authenticator switch, as shown in Figure 8-4.

- **Auto enablement**: Automatically enables trunk configuration on the authenticator switch, allowing user traffic from multiple VLANs coming from supplicant switches. Configure the `cisco-av-pair` as `device-traffic-class=switch` at the ACS. (You can configure this under the `group` or the `user` settings.)

**Figure 8-4 Authenticator and Supplicant Switch using CISP**

<table>
<thead>
<tr>
<th></th>
<th>Workstations (clients)</th>
<th>2</th>
<th>Supplicant switch (outside wiring closet)</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Authenticator switch</td>
<td>4</td>
<td>Access control server (ACS)</td>
</tr>
<tr>
<td>5</td>
<td>Trunk port</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Guidelines**

- You can configure NEAT ports with the same configurations as the other authentication ports. When the supplicant switch authenticates, the port mode is changed from `access` to `trunk` based on the switch vendor-specific attributes (VSAs). (`device-traffic-class=switch`).

- The VSA changes the authenticator switch port mode from access to trunk and enables 802.1x trunk encapsulation and the access VLAN if any would be converted to a native trunk VLAN. VSA does not change any of the port configurations on the supplicant.

- To change the host mode and apply a standard port configuration on the authenticator switch port, you can also use AutoSmart ports user-defined macros, instead of the switch VSA. This allows you to remove unsupported configurations on the authenticator switch port and to change the port mode from `access` to `trunk`. For more information, see Chapter 10, “Configuring Smartports Macros”.

For more information, see the “Configuring an Authenticator and a Supplicant Switch with NEAT” section on page 8-31.
Common Session ID

Authentication manager uses a single session ID (referred to as a common session ID) for a client no matter which authentication method is used. This ID is used for all reporting purposes, such as the show commands and MIBs. The session ID appears with all per-session syslog messages.

The session ID includes:

- The IP address of the Network Access Device (NAD)
- A monotonically increasing unique 32 bit integer
- The session start time stamp (a 32 bit integer)

This example shows how the session ID appears in the output of the show authentication command. The session ID in this example is 16000005000000B288508E5:

```
Switch# show authentication sessions
Interface   MAC Address   Method  Domain  Status        Session ID
Fa4/0/4     0000.0000.0203  mab    DATA   Authz Success  16000005000000B288508E5
```

This is an example of how the session ID appears in the syslog output. The session ID in this example is also 16000005000000B288508E5:

```
1w0d: %AUTHMGR-5-START: Starting 'mab' for client (0000.0000.0203) on Interface Fa4/0/4
AuditSessionID 16000005000000B288508E5
1w0d: %MAB-5-SUCCESS: Authentication successful for client (0000.0000.0203) on Interface Fa4/0/4 AuditSessionID 16000005000000B288508E5
1w0d: %AUTHMGR-7-RESULT: Authentication result 'success' from 'mab' for client (0000.0000.0203) on Interface Fa4/0/4 AuditSessionID 16000005000000B288508E5
```

The session ID is used by the NAD, the AAA server, and other report-analyzing applications to identify the client. The ID appears automatically. No configuration is required.

Configuring IEEE 802.1x Authentication

These sections describe how to configure IEEE 802.1x port-based authentication on your switch:

- Default 802.1x Configuration, page 8-15
- 802.1x Configuration Guidelines, page 8-16
- Configuring 802.1x Readiness Check, page 8-17 (optional)
- Configuring IEEE 802.1x Violation Modes, page 8-18
- Configuring IEEE 802.1x Authentication, page 8-19 (required)
- Configuring the Switch-to-RADIUS-Server Communication, page 8-20 (required)
- Configuring Periodic Re-Authentication, page 8-22 (optional)
- Manually Re-Authenticating a Client Connected to a Port, page 8-22 (optional)
- Changing the Quiet Period, page 8-22 (optional)
- Changing the Switch-to-Client Retransmission Time, page 8-23 (optional)
- Setting the Switch-to-Client Frame-Retransmission Number, page 8-24 (optional)
- Setting the Re-Authentication Number, page 8-25 (optional)
- Configuring the Host Mode, page 8-25 (optional)
- Configuring a Guest VLAN, page 8-26 (optional)
Default 802.1x Configuration

Table 8-1 shows the default IEEE 802.1x configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication, authorization, and accounting (AAA)</td>
<td>Disabled.</td>
</tr>
<tr>
<td>RADIUS server</td>
<td></td>
</tr>
<tr>
<td>• IP address</td>
<td>• None specified.</td>
</tr>
<tr>
<td>• UDP authentication port</td>
<td>• 1812.</td>
</tr>
<tr>
<td>• Key</td>
<td>• None specified.</td>
</tr>
<tr>
<td>Switch IEEE 802.1x enable state</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Per-port IEEE 802.1x enable state</td>
<td>Disabled (force-authorized). The port sends and receives normal traffic without IEEE 802.1x-based authentication of the client.</td>
</tr>
<tr>
<td>Periodic re-authentication</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Number of seconds between re-authentication attempts</td>
<td>3600 seconds.</td>
</tr>
<tr>
<td>Re-authentication number</td>
<td>2 times (number of times that the switch restarts the authentication process before the port changes to the unauthorized state).</td>
</tr>
<tr>
<td>Quiet period</td>
<td>60 seconds (number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client).</td>
</tr>
<tr>
<td>Retransmission time</td>
<td>30 seconds (number of seconds that the switch should wait for a response to an EAP request/identity frame from the client before resending the request).</td>
</tr>
<tr>
<td>Maximum retransmission number</td>
<td>2 times (number of times that the switch will send an EAP-request/identity frame before restarting the authentication process).</td>
</tr>
<tr>
<td>Host mode</td>
<td>Single-host mode.</td>
</tr>
<tr>
<td>Guest VLAN</td>
<td>None specified.</td>
</tr>
<tr>
<td>Restricted VLAN</td>
<td>None specified.</td>
</tr>
</tbody>
</table>
802.1x Configuration Guidelines

These are the IEEE 802.1x authentication configuration guidelines:

- When IEEE 802.1x is enabled, ports are authenticated before any other Layer 2 or Layer 3 features are enabled.

- The IEEE 802.1x protocol is supported on Layer 2 static-access ports, voice VLAN ports, and Layer 3 routed ports, but it is not supported on these port types:
  - Trunk port—If you try to enable IEEE 802.1x on a trunk port, an error message appears, and IEEE 802.1x is not enabled. If you try to change the mode of an IEEE 802.1x-enabled port to trunk, an error message appears, and the port mode is not changed.
  - Dynamic ports—A port in dynamic mode can negotiate with its neighbor to become a trunk port. If you try to enable IEEE 802.1x on a dynamic port, an error message appears, and IEEE 802.1x is not enabled. If you try to change the mode of an IEEE 802.1x-enabled port to dynamic, an error message appears, and the port mode is not changed.
  - Dynamic-access ports—If you try to enable IEEE 802.1x on a dynamic-access (VLAN Query Protocol [VQP]) port, an error message appears, and IEEE 802.1x is not enabled. If you try to change an IEEE 802.1x-enabled port to dynamic VLAN assignment, an error message appears, and the VLAN configuration is not changed.
  - EtherChannel port—Do not configure a port that is an active member of an EtherChannel as an IEEE 802.1x port. If IEEE 802.1x is enabled on a not-yet active port of an EtherChannel, the port does not join the EtherChannel.

Note

In software releases earlier than Cisco IOS Release 12.2(25)EY, if IEEE 802.1x is enabled on a not-yet active port of an EtherChannel, the port does not join the EtherChannel.

- Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) destination ports—You can enable IEEE 802.1x on a port that is a SPAN or RSPAN destination port. However, IEEE 802.1x is disabled until the port is removed as a SPAN or RSPAN destination port. You can enable IEEE 802.1x on a SPAN or RSPAN source port.

- You can configure any VLAN except an RSPAN VLAN or a voice VLAN as an IEEE 802.1x guest VLAN. The guest VLAN feature is not supported on internal VLANS (routed ports) or trunk ports; it is supported only on access ports.
Chapter 8 Configuring IEEE 802.1x Port-Based Authentication

Configuring IEEE 802.1x Authentication

- When IEEE 802.1x is enabled on a port, you cannot configure a port VLAN that is equal to a voice VLAN.
- The IEEE 802.1x with VLAN assignment feature is not supported on trunk ports, dynamic ports, or with dynamic-access port assignment through a VMPS.
- You can configure any VLAN except an RSPAN VLAN, a primary private VLAN, or a voice VLAN as an IEEE 802.1x restricted VLAN. The restricted VLAN feature is not supported on internal VLANs (routed ports) or trunk ports; it is supported only on access ports.
- You can configure IEEE 802.1x on a private-VLAN port, but do not configure IEEE 802.1x with port security, a voice VLAN, a guest VLAN, a restricted VLAN, or a per-user ACL on private-VLAN ports.

Maximum Number of Allowed Devices Per Port

This is the maximum number of devices allowed on an IEEE 802.1x-enabled port:

- In single-host mode, only one device is allowed on the access VLAN. If the port is also configured with a voice VLAN, an unlimited number of Cisco IP phones can send and receive traffic through the voice VLAN.
- In multidomain authentication (MDA) mode, one device is allowed for the access VLAN, and one IP phone is allowed for the voice VLAN.
- In multihost mode, only one IEEE 802.1x supplicant is allowed on the port, but an unlimited number of non-IEEE 802.1x hosts are allowed on the access VLAN. An unlimited number of devices are allowed on the voice VLAN.

Configuring 802.1x Readiness Check

The 802.1x readiness check monitors IEEE 802.1x activity on all the switch ports and displays information about the devices connected to the ports that support IEEE 802.1x. You can use this feature to determine if the devices connected to the switch ports are IEEE 802.1x-capable.

The 802.1x readiness check is allowed on all ports that can be configured for IEEE 802.1x. The readiness check is not available on a port that is configured as dot1x force-unauthorized.

Follow these guidelines to enable the readiness check on the switch:

- The readiness check is typically used before IEEE 802.1x is enabled on the switch.
- If you use the dot1x test eapol-capable privileged EXEC command without specifying an interface, all the ports on the switch stack are tested.
- When you configure the dot1x test eapol-capable command on an IEEE 802.1x-enabled port, and the link comes up, the port queries the connected client about its IEEE 802.1x capability. When the client responds with a notification packet, it is IEEE 802.1x-capable. A syslog message is generated if the client responds within the timeout period. If the client does not respond to the query, the client is not IEEE 802.1x-capable. No syslog message is generated.
- The readiness check can be sent on a port that handles multiple hosts (for example, a PC that is connected to an IP phone). A syslog message is generated for each of the clients that respond to the readiness check within the timer period.
Beginning in privileged EXEC mode, follow these steps to enable the IEEE 802.1x readiness check on the switch:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><strong>dot1x test eapol-capable [interface interface-id]</strong></td>
</tr>
<tr>
<td>Step 2</td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td>Step 3</td>
<td><strong>dot1x test timeout timeout</strong></td>
</tr>
<tr>
<td>Step 4</td>
<td><strong>end</strong></td>
</tr>
<tr>
<td></td>
<td><strong>show running-config</strong></td>
</tr>
</tbody>
</table>

This example shows how to enable a readiness check on a switch to query a port. It also shows the response received from the queried port verifying that the device connected to it is IEEE 802.1x-capable:

```
switch# dot1x test eapol-capable interface gigabitethernet1/0/13

DOT1X_PORT_EAPOL_CAPABLE:DOT1X: MAC 00-01-02-4b-f1-a3 on gigabitethernet1/0/13 is EAPOL capable
```

### Configuring IEEE 802.1x Violation Modes

You can configure an IEEE 802.1x port so that it shuts down, generates a syslog error, or discards packets from a new device when:

- a device connects to an IEEE 802.1x-enable port
- the maximum number of allowed about devices have been authenticated on the port

Beginning in privileged EXEC mode, follow these steps to configure the security violation actions on the switch:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td>Step 2</td>
<td><strong>aaa new-model</strong></td>
</tr>
<tr>
<td>Step 3</td>
<td><strong>aaa authentication dot1x [default] method1</strong></td>
</tr>
</tbody>
</table>
Configuring IEEE 802.1x Port-Based Authentication

To configure IEEE 802.1x port-based authentication, you must enable AAA and specify the authentication method list. A method list describes the sequence and authentication methods to be queried to authenticate a user.

The software uses the first method listed to authenticate users. If that method fails to respond, the software selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this cycle, the authentication process stops, and no other authentication methods are attempted.

To allow per-user ACLs or VLAN assignment, you must enable AAA authorization to configure the switch for all network-related service requests.

Beginning in privileged EXEC mode, follow these steps to configure IEEE 802.1x port-based authentication. This procedure is required.

---

**Command** | **Purpose**
--- | ---
**Step 4** | 
interface interface-id | Specify the port connected to the client that is to be enabled for IEEE 802.1x authentication, and enter interface configuration mode.

**Step 5** | 
switchport mode access | Set the port to access mode.

**Step 6** | 
dot1x violation-mode {shutdown | restrict | protect} | Configure the violation mode. The keywords have these meanings:
- shutdown—Error disable the port.
- restrict—Generate a syslog error.
- protect—Drop packets from any new device that sends traffic to the port.

**Step 7** | 
end | Return to privileged EXEC mode.

**Step 8** | 
show dot1x | Verify your entries.

**Step 9** | 
copy running-config startup-config | (Optional) Save your entries in the configuration file.

---

**Configuring IEEE 802.1x Authentication**

To configure IEEE 802.1x port-based authentication, you must enable AAA and specify the authentication method list. A method list describes the sequence and authentication methods to be queried to authenticate a user.

The software uses the first method listed to authenticate users. If that method fails to respond, the software selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this cycle, the authentication process stops, and no other authentication methods are attempted.

To allow per-user ACLs or VLAN assignment, you must enable AAA authorization to configure the switch for all network-related service requests.

Beginning in privileged EXEC mode, follow these steps to configure IEEE 802.1x port-based authentication. This procedure is required.

---

**Command** | **Purpose**
--- | ---
**Step 1** | 
configure terminal | Enter global configuration mode.

**Step 2** | 
aaa new-model | Enable AAA.

**Step 3** | 
aaa authentication dot1x {default} method1 [method2...]

Create an IEEE 802.1x authentication method list.

To create a default list that is used when a named list is not specified in the **authentication** command, use the **default** keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all ports.

Enter at least one of these keywords:
- group radius—Use the list of all RADIUS servers for authentication.
- none—Use no authentication. The client is automatically authenticated by the switch without using the information supplied by the client.

**Step 4** | 
dot1x system-auth-control | Enable IEEE 802.1x authentication globally on the switch.
### Step 5

**Command:**

```
aaa authorization network {default} group radius
```

**Purpose:**

(Optional) Configure the switch for user RADIUS authorization for all network-related service requests, such as per-user ACLs or VLAN assignment.

**Note:** For per-user ACLs, single-host mode must be configured. This setting is the default.

### Step 6

**Command:**

```
interface interface-id
```

**Purpose:**

Specify the port connected to the client that is to be enabled for IEEE 802.1x authentication, and enter interface configuration mode.

### Step 7

**Command:**

```
dot1x port-control auto
```

**Purpose:**

Enable IEEE 802.1x authentication on the port.

For feature interaction information, see the “802.1x Configuration Guidelines” section on page 8-16.

### Step 8

**Command:**

```
end
```

**Purpose:**

Return to privileged EXEC mode.

### Step 9

**Command:**

```
show dot1x
```

**Purpose:**

Verify your entries.

### Step 10

**Command:**

```
copy running-config startup-config
```

**Purpose:**

(Optional) Save your entries in the configuration file.

To disable AAA, use the `no aaa new-model` global configuration command. To disable 802.1x AAA authentication, use the `no aaa authentication dot1x {default | list-name}` global configuration command. To disable 802.1x AAA authorization, use the `no aaa authorization` global configuration command. To disable 802.1x authentication on the switch, use the `no dot1x system-auth-control` global configuration command.

This example shows how to enable AAA and 802.1x on a port:

```
Switch# configure terminal
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius
Switch(config)# dot1x system-auth-control
Switch(config)# interface fastethernet/0/1
Switch(config)# switchport mode access
Switch(config-if)# dot1x port-control auto
Switch(config-if)# end
```

### Configuring the Switch-to-RADIUS-Server Communication

RADIUS security servers are identified by their hostname or IP address, hostname and specific UDP port numbers, or IP address and specific UDP port numbers. The combination of the IP address and UDP port number creates a unique identifier, which enables RADIUS requests to be sent to multiple UDP ports on a server at the same IP address. If two different host entries on the same RADIUS server are configured for the same service—for example, authentication—the second host entry configured acts as the fail-over backup to the first one. The RADIUS host entries are tried in the order that they were configured.
Beginning in privileged EXEC mode, follow these steps to configure the RADIUS server parameters on the switch. This procedure is required.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>radius-server host {hostname</td>
<td>Configure the RADIUS server parameters. (ip-address)} auth-port port-number key string</td>
</tr>
<tr>
<td>3</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>4</td>
<td>show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>5</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To delete the specified RADIUS server, use the no radius-server host \(hostname \(ip-address\)\) global configuration command.

This example shows how to specify the server with IP address 172.20.39.46 as the RADIUS server, to use port 1612 as the authorization port, and to set the encryption key to rad123, matching the key on the RADIUS server:

```
Switch(config)# radius-server host 172.120.39.46 auth-port 1612 key rad123
```

You can globally configure the timeout, retransmission, and encryption key values for all RADIUS servers by using the radius-server host global configuration command. If you want to configure these options on a per-server basis, use the radius-server timeout, radius-server retransmit, and the radius-server key global configuration commands. For more information, see the “Configuring Settings for All RADIUS Servers” section on page 7-28.

You also need to configure some settings on the RADIUS server. These settings include the IP address of the switch and the key string to be shared by both the server and the switch. For more information, see the RADIUS server documentation.
Configuring Periodic Re-Authentication

You can enable periodic 802.1x client re-authentication and specify how often it occurs. If you do not specify a time period before enabling re-authentication, the number of seconds between re-authentication attempts is 3600.

Beginning in privileged EXEC mode, follow these steps to enable periodic re-authentication of the client and to configure the number of seconds between re-authentication attempts. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id Specify the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>dot1x reauthentication Enable periodic re-authentication of the client, which is disabled by default.</td>
</tr>
<tr>
<td>Step 4</td>
<td>dot1x timeout reauth-period seconds Set the number of seconds between re-authentication attempts. The range is 1 to 65535; the default is 3600 seconds. This command affects the behavior of the switch only if periodic re-authentication is enabled.</td>
</tr>
<tr>
<td>Step 5</td>
<td>end Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 6</td>
<td>show dot1x interface interface-id Verify your entries.</td>
</tr>
<tr>
<td>Step 7</td>
<td>copy running-config startup-config (Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable periodic re-authentication, use the no dot1x reauthentication interface configuration command. To return to the default number of seconds between re-authentication attempts, use the no dot1x timeout reauth-period interface configuration command.

This example shows how to enable periodic re-authentication and set the number of seconds between re-authentication attempts to 4000:

```
Switch(config-if)# dot1x reauthentication
Switch(config-if)# dot1x timeout reauth-period 4000
```

Manually Re-Authenticating a Client Connected to a Port

You can manually re-authenticate the client connected to a specific port at any time by entering the dot1x re-authenticate interface interface-id privileged EXEC command. This step is optional. If you want to enable or disable periodic re-authentication, see the “Configuring Periodic Re-Authentication” section on page 8-22.

This example shows how to manually re-authenticate the client connected to a port:

```
Switch# dot1x re-authenticate interface fastethernet1/0/1
```

Changing the Quiet Period

When the switch cannot authenticate the client, the switch remains idle for a set period of time and then tries again. The dot1x timeout quiet-period interface configuration command controls the idle period. A failed authentication of the client might occur because the client provided an invalid password. You can provide a faster response time to the user by entering a smaller number than the default.
Beginning in privileged EXEC mode, follow these steps to change the quiet period. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Specify the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3 dot1x timeout quiet-period seconds</td>
<td>Set the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client. The range is 1 to 65535 seconds; the default is 60.</td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5 show dot1x interface interface-id</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 6 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default quiet time, use the `no dot1x timeout quiet-period` interface configuration command.

This example shows how to set the quiet time on the switch to 30 seconds:

```
Switch(config-if)# dot1x timeout quiet-period 30
```

### Changing the Switch-to-Client Retransmission Time

The client responds to the EAP-request/identity frame from the switch with an EAP-response/identity frame. If the switch does not receive this response, it waits a set period of time (known as the retransmission time) and then resends the frame.

**Note**

You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Beginning in privileged EXEC mode, follow these steps to change the amount of time that the switch waits for client notification. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Specify the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3 dot1x timeout tx-period seconds</td>
<td>Set the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before resending the request. The range is 1 to 65535 seconds; the default is 30.</td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5 show dot1x interface interface-id</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 6 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default retransmission time, use the `no dot1x timeout tx-period` interface configuration command.
This example shows how to set 60 as the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before resending the request:

```
Switch(config-if)# dot1x timeout tx-period 60
```

### Setting the Switch-to-Client Frame-Retransmission Number

In addition to changing the switch-to-client retransmission time, you can change the number of times that the switch sends an EAP-request/identity frame (assuming no response is received) to the client before restarting the authentication process.

**Note**

You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Beginning in privileged EXEC mode, follow these steps to set the switch-to-client frame-retransmission number. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> interface interface-id</td>
<td>Specify the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong> dot1x max-reauth-req count</td>
<td>Set the number of times that the switch sends an EAP-request/identity frame to the client before restarting the authentication process. The range is 1 to 10; the default is 2.</td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 5</strong> show dot1x interface interface-id</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td><strong>Step 6</strong> copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default retransmission number, use the `no dot1x max-req` interface configuration command.

This example shows how to set 5 as the number of times that the switch sends an EAP-request/identity request before restarting the authentication process:

```
Switch(config-if)# dot1x max-req 5
```
Setting the Re-Authentication Number

You can also change the number of times that the switch restarts the authentication process before the port changes to the unauthorized state.

**Note**

You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Beginning in privileged EXEC mode, follow these steps to set the re-authentication number. This procedure is optional.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>configure terminal</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>interface interface-id</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Specify the port to be configured, and enter interface configuration mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>dot1x max-reauth-req count</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Set the number of times that the switch restarts the authentication process before the port changes to the unauthorized state. The range is 1 to 10; the default is 2.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>end</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Return to privileged EXEC mode.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>show dot1x interface interface-id</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Verify your entries.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>copy running-config startup-config</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(Optional) Save your entries in the configuration file.</td>
<td></td>
</tr>
</tbody>
</table>

To return to the default re-authentication number, use the `no dot1x max-reauth-req` interface configuration command.

This example shows how to set 4 as the number of times that the switch restarts the authentication process before the port changes to the unauthorized state:

```
Switch(config-if)# dot1x max-reauth-req 4
```

Configuring the Host Mode

You can configure an 802.1x port for single-host or for multiple-hosts mode. In single-host mode, only one host is allowed on an 802.1x port. When the host is authenticated, the port is placed in the authorized state. When the host leaves the port, the port becomes unauthorized. Packets from hosts other than the authenticated one are dropped.

You can attach multiple hosts to a single 802.1x-enabled port as shown in Figure 8-3 on page 8-6. In this mode, only one of the attached hosts must be successfully authorized for all hosts to be granted network access. If the port becomes unauthorized (re-authentication fails or an EAPOL-logoff message is received), all attached clients are denied access to the network.

With the multiple-hosts mode enabled, you can use 802.1x to authenticate the port and port security to manage network access for all MAC addresses, including that of the client.
Chapter 8      Configuring IEEE 802.1x Port-Based Authentication

Beginning in privileged EXEC mode, follow these steps to allow multiple hosts (clients) on an IEEE 802.1x-authorized port that has the `dot1x port-control` interface configuration command set to `auto`. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Specify the port to which multiple hosts are indirectly attached, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3 dot1x host-mode multi-host</td>
<td>Allow multiple hosts (clients) on an 802.1x-authorized port. Make sure that the <code>dot1x port-control</code> interface configuration command set is set to <code>auto</code> for the specified port.</td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5 show dot1x interface interface-id</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 6 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Enter the `dot1x host-mode single-host` interface configuration command to set the interface to allow a single host on the port.

**Note**
Although visible in the command-line interface help, the `dot1x host-mode multi-domain` interface configuration command is not supported. Configuring this command on an interface causes the interface to go into the error-disabled state.

To disable multiple hosts on the port, use the `no dot1x host-mode multi-host` interface configuration command.

This example shows how to enable 802.1x on a port and to allow multiple hosts:

```
Switch(config)# interface fastethernet1/0/1
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-host
```

### Configuring a Guest VLAN

When you configure a guest VLAN, clients that are not 802.1x-capable are put into the guest VLAN when the server does not receive a response to its EAP request/identity frame. Clients that are 802.1x-capable but fail authentication are not granted access to the network. The switch supports guest VLANs in single-host or multiple-hosts mode.

Beginning in privileged EXEC mode, follow these steps to configure a guest VLAN. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Specify the port to be configured, and enter interface configuration mode. For the supported port types, see the “802.1x Configuration Guidelines” section on page 8-16.</td>
</tr>
</tbody>
</table>
Chapter 8      Configuring IEEE 802.1x Port-Based Authentication

Configuring IEEE 802.1x Port-Based Authentication

To disable and remove the guest VLAN, use the no dot1x guest-vlan interface configuration command. If the port is currently authorized in the guest VLAN, the port returns to the unauthorized state.

This example shows how to enable VLAN 2 as an 802.1x guest VLAN on a port:

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# dot1x guest-vlan 2
```

Configuring a Restricted VLAN

When you configure a restricted VLAN on a switch, clients that are IEEE 802.1x-compliant are moved into the restricted VLAN when the authentication server does not receive a valid username and password. The switch supports restricted VLANs only in single-host mode.

Beginning in privileged EXEC mode, follow these steps to configure a restricted VLAN. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>switchport mode access</td>
</tr>
<tr>
<td></td>
<td>switchport mode private-vlan host</td>
</tr>
<tr>
<td>Step 4</td>
<td>dot1x port-control auto</td>
</tr>
<tr>
<td>Step 5</td>
<td>dot1x auth-fail vlan vlan-id</td>
</tr>
<tr>
<td>Step 6</td>
<td>end</td>
</tr>
<tr>
<td>Step 7</td>
<td>show dot1x interface interface-id</td>
</tr>
<tr>
<td>Step 8</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To disable and remove the restricted VLAN, use the no dot1x auth-fail vlan interface configuration command. The port returns to the unauthorized state.
This example shows how to enable VLAN 2 as an 802.1x restricted VLAN:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# dot1x auth-fail vlan 2
```

Use the `dot1x auth-fail max-attempts` interface configuration command to configure the maximum number of authentication attempts allowed before a user is assigned to the restricted VLAN. The range of allowable authentication attempts is 1 to 3. The default is 3 attempts.

Beginning in privileged EXEC mode, follow these steps to configure the maximum number of allowed authentication attempts. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Specify the port to be configured, and enter interface configuration mode. For the supported port types, see the “802.1x Configuration Guidelines” section on page 10-18.</td>
</tr>
<tr>
<td>Step 3 switchport mode access</td>
<td>Set the port to access mode, or</td>
</tr>
<tr>
<td>or</td>
<td>Configure the Layer 2 port as a private-VLAN host port.</td>
</tr>
<tr>
<td>Step 4 dot1x port-control auto</td>
<td>Enable 802.1x authentication on the port.</td>
</tr>
<tr>
<td>Step 5 dot1x auth-fail vlan vlan-id</td>
<td>Specify an active VLAN as an 802.1x restricted VLAN. The range is 1 to 4094. You can configure any active VLAN except an internal VLAN (routed port), an RSPAN VLAN, a primary private VLAN, or a voice VLAN as an 802.1x restricted VLAN.</td>
</tr>
<tr>
<td>Step 6 dot1x auth-fail max-attempts max attempts</td>
<td>Specify a number of authentication attempts to allow before a port moves to the restricted VLAN. The range is 1 to 3, and the default is 3.</td>
</tr>
<tr>
<td>Step 7 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 8 show dot1x interface interface-id</td>
<td>(Optional) Verify your entries.</td>
</tr>
<tr>
<td>Step 9 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default value, use the `no dot1x auth-fail max-attempts` interface configuration command.

This example shows how to set 2 as the number of authentication attempts allowed before the port moves to the restricted VLAN:

```
Switch(config-if)# dot1x auth-fail max-attempts
```
Chapter 8  Configuring IEEE 802.1x Port-Based Authentication

Resetting the 802.1x Configuration to the Default Values

Beginning in privileged EXEC mode, follow these steps to reset the 802.1x configuration to the default values. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2: interface interface-id</td>
<td>Specify the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3: dot1x default</td>
<td>Reset the configurable 802.1x parameters to the default values.</td>
</tr>
<tr>
<td>Step 4: end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5: show dot1x interface interface-id</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 6: copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Configuring 802.1x Accounting

Enabling AAA system accounting with 802.1x accounting allows system reload events to be sent to the accounting RADIUS server for logging. The server can then infer that all active 802.1x sessions are closed.

Because RADIUS uses the unreliable UDP transport protocol, accounting messages might be lost due to poor network conditions. If the switch does not receive the accounting response message from the RADIUS server after a configurable number of retransmissions of an accounting request, this system message appears:

Accounting message %s for session %s failed to receive Accounting Response.

When the stop message is not sent successfully, this message appears:

00:09:55: %RADIUS-4-RADIUS_DEAD: RADIUS server 172.20.246.201:1645,1646 is not responding.

Note

You must configure the RADIUS server to perform accounting tasks, such as logging start, stop, and interim-update messages and time stamps. To turn on these functions, enable logging of “Update/Watchdog packets from this AAA client” in your RADIUS server Network Configuration tab. Next, enable “CVS RADIUS Accounting” in your RADIUS server System Configuration tab.

Beginning in privileged EXEC mode, follow these steps to configure 802.1x accounting after AAA is enabled on your switch. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2: aaa accounting dot1x default start-stop group radius</td>
<td>Enable 802.1x accounting using the list of all RADIUS servers.</td>
</tr>
<tr>
<td>Step 3: aaa accounting system default start-stop group radius</td>
<td>(Optional) Enables system accounting (using the list of all RADIUS servers) and generates system accounting reload event messages when the switch reloads.</td>
</tr>
<tr>
<td>Step 4: end</td>
<td>Return to privileged EXEc mode.</td>
</tr>
</tbody>
</table>
Chapter 8  Configuring IEEE 802.1x Port-Based Authentication

Configuring IEEE 802.1x Authentication

Use the `show radius statistics` privileged EXEC command to display the number of RADIUS messages that do not receive the accounting response message.

This example shows how to configure 802.1x accounting. The first command configures the RADIUS server, specifying 1813 as the UDP port for accounting:

```
Switch(config)# radius-server host 172.120.39.46 auth-port 1812 acct-port 1813 key rad123
Switch(config)# aaa accounting dot1x default start-stop group radius
Switch(config)# aaa accounting system default start-stop group radius
```

Configuring 802.1x User Distribution

Beginning in global configuration, follow these steps to configure a VLAN group and to map a VLAN to it:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong> show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td><strong>Step 6</strong> copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Use the `show radius statistics` privileged EXEC command to display the number of RADIUS messages that do not receive the accounting response message.

This example shows how to configure 802.1x accounting. The first command configures the RADIUS server, specifying 1813 as the UDP port for accounting:

```
Switch(config)# radius-server host 172.120.39.46 auth-port 1812 acct-port 1813 key rad123
Switch(config)# aaa accounting dot1x default start-stop group radius
Switch(config)# aaa accounting system default start-stop group radius
```

### Configuring 802.1x User Distribution

Beginning in global configuration, follow these steps to configure a VLAN group and to map a VLAN to it:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> vlan group vlan-group-name vlan-list vlan-list</td>
<td>Configure a VLAN group, and map a single VLAN or a range of VLANs to it.</td>
</tr>
<tr>
<td><strong>Step 2</strong> show vlan group all vlan-group-name</td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td><strong>Step 3</strong> no vlan group vlan-group-name vlan-list vlan-list</td>
<td>Clear the VLAN group configuration or elements of the VLAN group configuration.</td>
</tr>
</tbody>
</table>

This example shows how to configure the VLAN groups, to map the VLANs to the groups, to and verify the VLAN group configurations and mapping to the specified VLANs:

```
switch(config)# vlan group eng-dept vlan-list 10
switch(config)# show vlan group group-name eng-dept
Group Name    Vlans Mapped
-----------    ----------
eng-dept      10
```

```
switch(config)# show vlan group all
Group Name    Vlans Mapped
-----------    ----------
eng-dept      10
hr-dept       20
```

This example shows how to add a VLAN to an existing VLAN group and to verify that the VLAN was added:

```
switch(config)# vlan group eng-dept vlan-list 30
switch(config)# show vlan group eng-dept
Group Name    Vlans Mapped
-----------    ----------
eng-dept      10, 30
```

This example shows how to remove a VLAN from a VLAN group:

```
switch# no vlan group eng-dept vlan-list 10
```
This example shows that when all the VLANs are cleared from a VLAN group, the VLAN group is cleared:

```
switch(config)# no vlan group eng-dept vlan-list 30
Vlan 30 is successfully cleared from vlan group eng-dept.
```

```
switch(config)# show vlan group group-name eng-dept
```

This example shows how to clear all the VLAN groups:

```
switch(config)# no vlan group end-dept vlan-list all
switch(config)# show vlan-group all
```

For more information about these commands, see the *Cisco IOS Security Command Reference*.

---

## Configuring an Authenticator and a Supplicant Switch with NEAT

Configuring this feature requires that one switch outside a wiring closet is configured as a supplicant and is connected to an authenticator switch.

For overview information, see the “802.1x Supplicant and Authenticator Switches with Network Edge Access Topology (NEAT)” section on page 8-12.

**Note**

The `cisco-av-pairs` must be configured as `device-traffic-class=switch` on the ACS, which sets the interface as a trunk after the supplicant is successfully authenticated.

Beginning in privileged EXEC mode, follow these steps to configure a switch as an authenticator:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>cisp enable</code></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>interface interface-id</code></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>switchport mode access</code></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>authentication port-control auto</code></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>dot1x pae authenticator</code></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><code>spanning-tree portfast</code></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><code>end</code></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td><code>show running-config interface interface-id</code></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td><code>copy running-config startup-config</code></td>
</tr>
</tbody>
</table>

This example shows how to configure a switch as an 802.1x authenticator:

```
Switch# configure terminal
Switch(config)# cisp enable
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# switchport mode access
Switch(config-if)# authentication port-control auto
Switch(config-if)# dot1x pae authenticator
```
Configuring IEEE 802.1x Port-Based Authentication

Switch(config-if)# spanning-tree portfast trunk

Beginning in privileged EXEC mode, follow these steps to configure a switch as a supplicant:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>cisp enable</td>
</tr>
<tr>
<td></td>
<td>Enable CISP.</td>
</tr>
<tr>
<td>Step 3</td>
<td>dot1x credentials profile</td>
</tr>
<tr>
<td></td>
<td>Create 802.1x credentials profile. This must be attached to the port that is configured as supplicant.</td>
</tr>
<tr>
<td>Step 4</td>
<td>username suppswitch</td>
</tr>
<tr>
<td></td>
<td>Create a username.</td>
</tr>
<tr>
<td>Step 5</td>
<td>password password</td>
</tr>
<tr>
<td></td>
<td>Create a password for the new username.</td>
</tr>
<tr>
<td>Step 6</td>
<td>dot1x supplicant force-multicast</td>
</tr>
<tr>
<td></td>
<td>Force the switch to send only multicast EAPOL packets when it receives either unicast or multicast packets. This also allows NEAT to work on the supplicant switch in all host modes.</td>
</tr>
<tr>
<td>Step 7</td>
<td>interface interface-id</td>
</tr>
<tr>
<td></td>
<td>Specify the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 8</td>
<td>switchport trunk encapsulation dot1q</td>
</tr>
<tr>
<td></td>
<td>Set the port to trunk mode.</td>
</tr>
<tr>
<td>Step 9</td>
<td>switchport mode trunk</td>
</tr>
<tr>
<td></td>
<td>Configure the interface as a VLAN trunk port.</td>
</tr>
<tr>
<td>Step 10</td>
<td>dot1x pae supplicant</td>
</tr>
<tr>
<td></td>
<td>Configure the interface as a port access entity (PAE) supplicant.</td>
</tr>
<tr>
<td>Step 11</td>
<td>dot1x credentials profile-name</td>
</tr>
<tr>
<td></td>
<td>Attach the 802.1x credentials profile to the interface.</td>
</tr>
<tr>
<td>Step 12</td>
<td>end</td>
</tr>
<tr>
<td></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 13</td>
<td>show running-config interface interface-id</td>
</tr>
<tr>
<td></td>
<td>Verify your configuration.</td>
</tr>
<tr>
<td>Step 14</td>
<td>copy running-config startup-config</td>
</tr>
<tr>
<td></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

This example shows how to configure a switch as a supplicant:

```
Switch# configure terminal
Switch(config)# cisp enable
Switch(config)# dot1x credentials test
Switch(config)# username suppswitch
Switch(config)# password myswitch
Switch(config)# dot1x supplicant force-multicast
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# dot1x pae supplicant
Switch(config-if)# dot1x credentials test
Switch(config-if)# end
```

Configuring NEAT with ASP

You can also use an AutoSmart Ports user-defined macro instead of the switch VSA to configure the authenticator switch. For more information, see the Chapter 10, “Configuring Smartports Macros.”
Configuring 802.1x Authentication with Downloadable ACLs and Redirect URLs

In addition to configuring 802.1x authentication on the switch, you need to configure the ACS. For more information, see the Cisco Secure ACS configuration guides.

**Note**

You must configure a downloadable ACL on the ACS before downloading it to the switch.

After authentication on the port, you can use the `show ip access-list` privileged EXEC command to display the downloaded ACLs on the port.

Configuring Downloadable ACLs

The policies take effect after client authentication and the client IP address addition to the IP device tracking table. The switch then applies the downloadable ACL to the port.

Beginning in privileged EXEC mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2: ip device tracking</td>
<td>Configure the ip device tracking table.</td>
</tr>
<tr>
<td>Step 3: aaa new-model</td>
<td>Enables AAA.</td>
</tr>
<tr>
<td>Step 4: aaa authorization network default group radius</td>
<td>Sets the authorization method to local. To remove the authorization method, use the <code>no aaa authorization network default group radius</code> command.</td>
</tr>
<tr>
<td>Step 5: radius-server vsa send authentication</td>
<td>Configure the radius vsa send authentication.</td>
</tr>
<tr>
<td>Step 6: interface interface-id</td>
<td>Specify the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 7: ip access-group acl-id in</td>
<td>Configure the default ACL on the port in the input direction. <strong>Note</strong> The <code>acl-id</code> is an access list name or number.</td>
</tr>
<tr>
<td>Step 8: show running-config interface interface-id</td>
<td>Verify your configuration.</td>
</tr>
<tr>
<td>Step 9: copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
# Configuring a Downloadable Policy

Beginning in privileged EXEC mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> access-list access-list-number deny source source-wildcard log</td>
<td>Defines the default port ACL by using a source address and wildcard. The access-list-number is a decimal number from 1 to 99 or 1300 to 1999. Enter deny or permit to specify whether to deny or permit access if conditions are matched. The source is the source address of the network or host that sends a packet, such as this:</td>
</tr>
<tr>
<td></td>
<td>• The 32-bit quantity in dotted-decimal format.</td>
</tr>
<tr>
<td></td>
<td>• The keyword any as an abbreviation for source and source-wildcard value of 0.0.0.0 255.255.255.255. You do not need to enter a source-wildcard value.</td>
</tr>
<tr>
<td></td>
<td>• The keyword host as an abbreviation for source and source-wildcard of source 0.0.0.0.</td>
</tr>
<tr>
<td></td>
<td>(Optional) Applies the source-wildcard wildcard bits to the source. (Optional) Enters log to cause an informational logging message about the packet that matches the entry to be sent to the console.</td>
</tr>
<tr>
<td><strong>Step 3</strong> interface interface-id</td>
<td>Enter interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong> ip access-group acl-id in</td>
<td>Configure the default ACL on the port in the input direction.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The acl-id is an access list name or number.</td>
</tr>
<tr>
<td><strong>Step 5</strong> exit</td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 6</strong> aaa new-model</td>
<td>Enables AAA.</td>
</tr>
<tr>
<td><strong>Step 7</strong> aaa authorization network default group radius</td>
<td>Sets the authorization method to local. To remove the authorization method, use the no aaa authorization network default group radius command.</td>
</tr>
<tr>
<td><strong>Step 8</strong> ip device tracking</td>
<td>Enables the IP device tracking table. To disable the IP device tracking table, use the no ip device tracking global configuration commands.</td>
</tr>
<tr>
<td><strong>Step 9</strong> ip device tracking probe [count</td>
<td>(Optional) Configures the IP device tracking table:</td>
</tr>
<tr>
<td>interval</td>
<td></td>
</tr>
<tr>
<td>use-svi]</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Command Purpose

<table>
<thead>
<tr>
<th>Step 10</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>radius-server vsa send authentication</td>
<td>Configures the network access server to recognize and use vendor-specific attributes.</td>
</tr>
<tr>
<td>Note</td>
<td></td>
<td>The downloadable ACL must be operational.</td>
</tr>
<tr>
<td>Step 11</td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 12</td>
<td>show ip device tracking all</td>
<td>Displays information about the entries in the IP device tracking table.</td>
</tr>
<tr>
<td>Step 13</td>
<td>copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
</tbody>
</table>

This example shows how to configure a switch for a downloadable policy:

```
Switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# aaa new-model
Switch(config)# aaa authorization network default group radius
Switch(config)# ip device tracking
Switch(config)# ip access-list extended default_acl
Switch(config-ext-nacl)# permit ip any any
Switch(config-ext-nacl)# exit
Switch(config)# radius-server vsa send authentication
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip access-group default_acl in
Switch(config-if)# exit
```

### Displaying 802.1x Statistics and Status

To display 802.1x statistics for all ports, use the `show dot1x all statistics` privileged EXEC command.

To display 802.1x statistics for a specific port, use the `show dot1x statistics interface interface-id` privileged EXEC command.

To display the 802.1x administrative and operational status for the switch, use the `show dot1x all` privileged EXEC command. To display the 802.1x administrative and operational status for a specific port, use the `show dot1x interface interface-id` privileged EXEC command.

For detailed information about the fields in these displays, see the command reference for this release.
Configuring Interface Characteristics

This chapter defines the types of interfaces on the Catalyst 3750 Metro switch and describes how to configure them.

The chapter has these sections:

- Understanding Interface Types, page 9-1
- Using Interface Configuration Mode, page 9-7
- Configuring Ethernet Interfaces, page 9-11
- Configuring Layer 3 Interfaces, page 9-17
- Configuring the System MTU, page 9-19
- Monitoring and Maintaining the Interfaces, page 9-22

For complete syntax and usage information for the commands used in this chapter, see the switch command reference for this release and the online Cisco IOS Interface Command Reference, Release 12.2.

Understanding Interface Types

This section describes the different types of interfaces supported by the switch with references to chapters that contain more detailed information about configuring these interface types. The rest of the chapter describes configuration procedures for physical interface characteristics.

These sections are included:

- Port-Based VLANs, page 9-2
- Switch Ports, page 9-2
- Routed Ports, page 9-4
- Switch Virtual Interfaces, page 9-4
- EtherChannel Port Groups, page 9-5
- Connecting Interfaces, page 9-5
Port-Based VLANs

A VLAN is a switched network that is logically segmented by function, team, or application, without regard to the physical location of the users. For more information about VLANs, see Chapter 11, “Configuring VLANs.” Packets received on a port are forwarded only to ports that belong to the same VLAN as the receiving port. Network devices in different VLANs cannot communicate with one another without a Layer 3 device to route traffic between the VLANs.

VLAN partitions provide hard firewalls for traffic in the VLAN, and each VLAN has its own MAC address table. A VLAN comes into existence when a local port is configured to be associated with the VLAN, when the VLAN Trunking Protocol (VTP) learns of its existence from a neighbor on a trunk, or when a user creates a VLAN.

To configure normal-range VLANs (VLAN IDs 1 to 1005), use the `vlan vlan-id` global configuration command to enter config-vlan mode or the `vlan database` privileged EXEC command to enter VLAN database configuration mode. The VLAN configurations for VLAN IDs 1 to 1005 are saved in the VLAN database. To configure extended-range VLANs (VLAN IDs 1006 to 4094), you must use config-vlan mode with VTP mode set to transparent. Extended-range VLANs are not added to the VLAN database. When VTP mode is transparent, the VTP and VLAN configuration is saved in the switch running configuration, and you can save it in the switch startup configuration file by entering the `copy running-config startup-config` privileged EXEC command.

Add ports to a VLAN by using the `switchport` interface configuration commands:

- Identify the interface.
- For a trunk port, set trunk characteristics, and if desired, define the VLANs to which it can belong.
- For an access port, set and define the VLAN to which it belongs.
- For a tunnel port, set and define the VLAN ID for the customer-specific VLAN tag. See Chapter 15, “Configuring IEEE 802.1Q and Layer 2 Protocol Tunneling.”

Switch Ports

Switch ports are Layer 2-only interfaces associated with a physical port. Switch ports belong to one or more VLANs. A switch port can be an access port, a trunk port, or a tunnel port. You can configure a port as an access port or trunk port or let the Dynamic Trunking Protocol (DTP) operate on a per-port basis to determine switchport mode by negotiating with the port on the other end of the link. You must manually configure tunnel ports as part of an asymmetric link connected to an 802.1Q trunk port. Switch ports are used for managing the physical interface and associated Layer 2 protocols and do not handle routing or bridging.

Configure switch ports by using the `switchport` interface configuration commands. For detailed information about configuring access port and trunk port characteristics, see Chapter 11, “Configuring VLANs.” For more information about tunnel ports, see Chapter 15, “Configuring IEEE 802.1Q and Layer 2 Protocol Tunneling.”

Access Ports

An access port belongs to and carries the traffic of only one VLAN (unless it is configured as a voice VLAN port). Traffic is received and sent in native formats with no VLAN tagging. Traffic arriving on an access port is assumed to belong to the VLAN assigned to the port. If an access port receives a tagged packet (Inter-Switch Link [ISL] or 802.1Q tagged), the packet is dropped, and the source address is not learned.
Understanding Interface Types

Note
ISL is not supported on the enhanced-services (ES) ports.

Two types of access ports are supported:

- Static access ports are manually assigned to a VLAN.
- VLAN membership of dynamic access ports is learned through incoming packets. By default, a dynamic access port is not a member of any VLAN, and forwarding to and from the port is enabled only when the VLAN membership of the port is discovered. Dynamic access ports on the switch are assigned to a VLAN by a VLAN Membership Policy Server (VMPS). The VMPS can be a Catalyst 6000 series switch; the Catalyst 3750 Metro switch cannot be a VMPS server.

You can also configure an access port with an attached Cisco IP Phone to use one VLAN for voice traffic and another VLAN for data traffic from a device attached to the phone. For more information about voice VLAN ports, see Chapter 14, “Configuring Voice VLAN.”

Trunk Ports

A trunk port carries the traffic of multiple VLANs and by default is a member of all VLANs in the VLAN database.

Note
Beginning with Cisco IOS Release 12.2(22)EY, on ES trunk ports, only 802.1Q encapsulation is supported. ES ports do not support ISL encapsulation.

Two types of standard trunk ports are supported:

- In an ISL trunk port, all received packets are expected to be encapsulated with an ISL header, and all transmitted packets are sent with an ISL header. Native (non-tagged) frames received from an ISL trunk port are dropped.
- An IEEE 802.1Q trunk port supports simultaneous tagged and untagged traffic. An 802.1Q trunk port is assigned a default Port VLAN ID (PVID), and all untagged traffic travels on the port default PVID. All untagged traffic and tagged traffic with a NULL VLAN ID are assumed to belong to the port default PVID. A packet with a VLAN ID equal to the outgoing port default PVID is sent untagged. All other traffic is sent with a VLAN tag.

Although by default, a trunk port is a member of every VLAN known to the VTP, you can limit VLAN membership by configuring an allowed list of VLANs for each trunk port. The list of allowed VLANs does not affect any other port but the associated trunk port. By default, all possible VLANs (VLAN ID 1 to 4094) are in the allowed list. A trunk port can only become a member of a VLAN if VTP knows of the VLAN and the VLAN is in the enabled state. If VTP learns of a new, enabled VLAN and the VLAN is in the allowed list for a trunk port, the trunk port automatically becomes a member of that VLAN and traffic is forwarded to and from the trunk port for that VLAN. If VTP learns of a new, enabled VLAN that is not in the allowed list for a trunk port, the port does not become a member of the VLAN, and no traffic for the VLAN is forwarded to or from the port.

For more information about trunk ports, see Chapter 11, “Configuring VLANs.”
Tunnel Ports

Tunnel ports are used in 802.1Q tunneling to segregate the traffic of customers in a service provider network from other customers who appear to be on the same VLAN. You configure an asymmetric link from a tunnel port on a service provider edge switch to an 802.1Q trunk port on the customer switch. Packets entering the tunnel port on the edge switch, already 802.1Q-tagged with the customer VLANs, are encapsulated with another layer of 802.1Q tag (called the metro tag) containing a VLAN ID unique in the service provider network for each customer. The double-tagged packets go through the service-provider network, keeping the original customer VLANs separate from those of other customers. At the outbound interface, also a tunnel port, the metro tag is removed, and the original VLAN numbers from the customer network are retrieved.

Tunnel ports cannot be trunk ports or access ports and must belong to a VLAN unique for each customer.

For more information about tunnel ports, see Chapter 15, “Configuring IEEE 802.1Q and Layer 2 Protocol Tunneling.”

Routed Ports

A routed port is a physical port that acts like a port on a router; it does not have to be connected to a router. A routed port is not associated with a particular VLAN, as is an access port. A routed port behaves like a regular router interface, except that it does not support VLAN subinterfaces. Routed ports can be configured with a Layer 3 routing protocol. A routed port is a Layer 3 interface only and does not support Layer 2 protocols, such as DTP and STP.

Configure routed ports by putting the interface into Layer 3 mode with the `no switchport` interface configuration command. Then assign an IP address to the port, enable routing, and assign routing protocol characteristics by using the `ip routing` and `router protocol` global configuration commands.

Caution

Entering a `no switchport` interface configuration command shuts down the interface and then re-enables it, which might generate messages on the device to which the interface is connected.

The number of routed ports that you can configure is not limited by software. However, the interrelationship between this number and the number of other features being configured might impact CPU performance because of hardware limitations. See the “Configuring Layer 3 Interfaces” section on page 9-17 for information about what happens when hardware resource limitations are reached.

For more information about IP unicast and multicast routing and routing protocols, see Chapter 36, “Configuring IP Unicast Routing,” and Chapter 45, “Configuring IP Multicast Routing.”

Switch Virtual Interfaces

A switch virtual interface (SVI) represents a VLAN of switch ports as one interface to the routing or bridging function in the system. Only one SVI can be associated with a VLAN, but you need to configure an SVI for a VLAN only when you wish to route between VLANs, to fallback-bridge nonroutable protocols between VLANs, or to provide IP host connectivity to the switch. By default, an SVI is created for the default VLAN (VLAN 1) to permit remote switch administration. Additional SVIs must be explicitly configured. SVIs provide IP host connectivity only to the system; in Layer 3 mode, you can configure routing across SVIs.
Although the switch stack supports a total or 1005 VLANs (and SVIs), the interrelationship between the number of SVIs and routed ports and the number of other features being configured might impact CPU performance because of hardware limitations. See the “Configuring Layer 3 Interfaces” section on page 9-17 for information about what happens when hardware resource limitations are reached.

SVIs are created the first time that you enter the \texttt{vlan} interface configuration command for a VLAN interface. The VLAN corresponds to the VLAN tag associated with data frames on an ISL or 802.1Q encapsulated trunk or the VLAN ID configured for an access port. Configure a VLAN interface for each VLAN for which you want to route traffic, and assign it an IP address. For more information, see the “Manually Assigning IP Information” section on page 3-14.

\underline{Note} 
When you create an SVI, it does not become active until it is associated with a physical port.

SVIs support routing protocols and bridging configurations. For more information about configuring IP routing, see Chapter 36, “Configuring IP Unicast Routing,” Chapter 45, “Configuring IP Multicast Routing,” and Chapter 47, “Configuring Fallback Bridging.”

\section*{EtherChannel Port Groups}

EtherChannel port groups provide the ability to treat multiple switch ports as one switch port. These port groups act as a single logical port for high-bandwidth connections between switches or between switches and servers. An EtherChannel balances the traffic load across the links in the channel. If a link within the EtherChannel fails, traffic previously carried over the failed link changes to the remaining links. You can group multiple trunk ports into one logical trunk port, group multiple access ports into one logical access port, group multiple tunnel ports into one logical tunnel port, or group multiple routed ports into one logical routed port. Most protocols operate over either single ports or aggregated switch ports and do not recognize the physical ports within the port group. Exceptions are the DTP, the Cisco Discovery Protocol (CDP), and the Port Aggregation Protocol (PAgP), which operate only on physical ports.

When you configure an EtherChannel, you create a port-channel logical interface and assign an interface to the EtherChannel. For Layer 3 interfaces, you manually create the logical interface by using the \texttt{interface port-channel} global configuration command. Then you manually assign an interface to the EtherChannel by using the \texttt{channel-group} interface configuration command. For Layer 2 interfaces, use the \texttt{channel-group} interface configuration command to dynamically create the port-channel logical interface. This command binds the physical and logical ports together. For more information, see Chapter 35, “Configuring EtherChannels and Link-State Tracking.”

\section*{Connecting Interfaces}

Devices within a single VLAN can communicate directly through any switch. Ports in different VLANs cannot exchange data without going through a routing device. With a standard Layer 2 switch, ports in different VLANs have to exchange information through a router. In the configuration shown in Figure 9-1, when Host A in VLAN 20 sends data to Host B in VLAN 30, it must go from Host A to the switch, to the router, back to the switch, and then to Host B.
By using the switch with routing enabled (as a Layer 3 switch), when you configure VLAN 20 and VLAN 30 each with an SVI to which an IP address is assigned, packets can be sent from Host A to Host B directly through the switch with no need for an external router (Figure 9-2).

The switch supports two methods of forwarding traffic between interfaces: routing and fallback bridging. Whenever possible, to maintain high performance, forwarding is done by the switch hardware. However, only IP Version 4 packets with Ethernet II encapsulation can be routed in hardware. Non-IP traffic and traffic with other encapsulation methods can be fallback-bridged by hardware.

- The routing function can be enabled on all SVIs and routed ports. The switch routes only IP traffic. When IP routing protocol parameters and address configuration are added to an SVI or routed port, any IP traffic received from these ports is routed. For more information, see Chapter 36, “Configuring IP Unicast Routing,” Chapter 45, “Configuring IP Multicast Routing,” and Chapter 46, “Configuring MSDP.”
Using Interface Configuration Mode

The switch supports these interface types:

- Physical ports—including switch ports and routed ports
- VLANs—switch virtual interfaces
- Port-channels—EtherChannel of interfaces

You can also configure a range of interfaces (see the “Configuring a Range of Interfaces” section on page 9-8).

To configure a physical interface (port), enter interface configuration mode, and specify the interface type switch number, module number, and switch port number.

- Type—Fast Ethernet (fastethernet or fa) for 10/100 Mb/s Ethernet or Gigabit Ethernet (gigabitethernet or gi) for small form-factor pluggable (SFP) Gigabit Ethernet interfaces.
- Switch number—For the Catalyst 3750 Metro switch, this number is always 1.
- Module number—The module or slot number on the switch. The module number is zero (0) for Fast Ethernet interfaces and standard SFP module interfaces or 1 for ES SFP module interfaces.
- Port number—The interface number on the switch. The port numbers always begin at 1, starting at the left when facing the front of the switch, for example, fastethernet 1/0/1, fastethernet 1/0/2. The numbers start again from 1 when the type of interface changes. The standard SFP module interfaces are gigabitethernet 1/0/1 and gigabitethernet 1/0/2, and the ES SFP module interfaces are gigabitethernet 1/1/1 and gigabitethernet 1/1/2.

You can identify physical interfaces by physically checking the interface location on the switch. You can also use the IOS `show` privileged EXEC commands to display information about a specific interface or all the interfaces on the switch. The remainder of this chapter primarily provides physical interface configuration procedures.

Procedures for Configuring Interfaces

These general instructions apply to all interface configuration processes.

**Step 1**

Enter the `configure terminal` command at the privileged EXEC prompt:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
```

**Step 2**

Enter the `interface` global configuration command. Identify the interface type and number. For physical interfaces, this includes the switch number (1) and the number of the port to be configured:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)#
```
You do not need to add a space between the physical interface type and the interface number. For example, in the preceding line, you can specify `gigabitethernet 1/0/1`, `gigabitethernet1/0/1`, `gi 1/0/1`, or `gi1/0/1`.

**Step 3** Follow each `interface` command with the interface configuration commands that the interface requires. The commands that you enter define the protocols and applications that will run on the interface. The commands are collected and applied to the interface when you enter another interface command or enter `end` to return to privileged EXEC mode.

You can also configure a range of interfaces by using the `interface range` or `interface range macro` global configuration commands. Interfaces configured in a range must be the same type and must be configured with the same feature options.

**Step 4** After you configure an interface, verify its status by using the `show` privileged EXEC commands listed in the “Monitoring and Maintaining the Interfaces” section on page 9-22.

Enter the `show interfaces` privileged EXEC command to see a list of all interfaces on or configured for the switch. A report is provided for each interface that the device supports or for the specified interface.

### Configuring a Range of Interfaces

You can use the `interface range` global configuration command to configure multiple interfaces with the same configuration parameters. When you enter the interface range configuration mode, all command parameters that you enter are attributed to all interfaces within that range until you exit this mode.

Beginning in privileged EXEC mode, follow these steps to configure a range of interfaces with the same parameters:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>`interface range {port-range</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>end</code></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>show interfaces [interface-id]</code></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>copy running-config startup-config</code></td>
</tr>
</tbody>
</table>
When using the **interface range** global configuration command, note these guidelines:

- **Valid entries for port-range:**
  - *vlan* vlan-ID - vlan-ID, where VLAN ID is from 1 to 4094
  - *fastethernet* switch/module/{first port} - {last port}, where switch is 1 and module is 0
  - *gigabitethernet* switch/module/{first port} - {last port}, where switch is 1 and module is 0 for the standard SFP module ports and 1 for the ES SFP module ports
  - *port-channel* port-channel-number - port-channel-number, where port-channel-number is from 1 to 12

**Note** When you use the **interface range** command with port channels, the first and last port channel number must be active port channels.

- You must add a space between the first interface number and the hyphen when using the **interface range** command. For example, the command **interface range fastethernet 1/0/1 - 5** is a valid range; the command **interface range fastethernet 1/0/1-5** is not a valid range.

- The **interface range** command only works with VLAN interfaces that have been configured with the **interface vlan** command. The **show running-config** privileged EXEC command displays the configured VLAN interfaces. VLAN interfaces not displayed by the **show running-config** command cannot be used with the **interface range** command.

- All interfaces defined as in a range must be the same type (all Fast Ethernet ports, all Gigabit Ethernet SFP module ports, all EtherChannel ports, or all VLANs), but you can enter multiple ranges in a command.

This example shows how to use the **interface range** global configuration command to set the speed on 10/100 ports 1 to 5 to 100 Mb/s:

```
Switch# configure terminal
Switch(config)# interface range fastethernet 1/0/1 - 5
Switch(config-if-range)# speed 100
```

This example shows how to use a comma to add different interface type strings to the range to enable Fast Ethernet ports in the range 1 to 3 and Gigabit Ethernet standard SFP module ports 1 and 2 to receive flow control pause frames:

```
Switch# configure terminal
Switch(config)# interface range fastethernet 1/0/1 - 3, gigabitethernet 1/0/1 - 2
Switch(config-if-range)# flowcontrol receive on
```

If you enter multiple configuration commands while you are in interface range mode, each command is executed as it is entered. The commands are not batched together and executed after you exit interface range mode. If you exit interface range configuration mode while the commands are being executed, some commands might not be executed on all interfaces in the range. Wait until the command prompt reappears before exiting interface range configuration mode.
Configuring and Using Interface Range Macros

You can create an interface range macro to automatically select a range of interfaces for configuration. Before you can use the macro keyword in the interface range macro global configuration command string, you must use the define interface-range global configuration command to define the macro.

Beginning in privileged EXEC mode, follow these steps to define an interface range macro:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>define interface-range macro_name interface-range</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>interface range macro macro_name</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
</tr>
<tr>
<td>Step 5</td>
<td>show running-config</td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

Use the no define interface-range macro_name global configuration command to delete a macro.

When using the define interface-range global configuration command, note these guidelines:

- Valid entries for interface-range:
  - **vlan** vlan-ID - vlan-ID, where VLAN ID is from 1 to 4094
  - **fastethernet** switch/module/[first port] - [last port], where switch is 1 and module is 0
  - **gigabitethernet** switch/module/[first port] - [last port], where switch is 1 and module is 0 for the standard SFP module ports and 1 for the ES SFP module ports.
  - **port-channel** port-channel-number - port-channel-number, where port-channel-number is from 1 to 12.

  **Note** When you use the interface ranges with port channels, the first and last port channel number must be active port channels.

- You must add a space between the first interface number and the hyphen when entering an interface-range. For example, **fastethernet 1/0/1 - 5** is a valid range; **fastethernet 1/0/1-5** is not a valid range.

- The VLAN interfaces must have been configured with the interface vlan command. The show running-config privileged EXEC command displays the configured VLAN interfaces. VLAN interfaces not displayed by the show running-config command cannot be used as interface-ranges.

- All interfaces defined as in a range must be the same type (all Fast Ethernet ports, all Gigabit Ethernet SFP module ports, all EtherChannel ports, or all VLANs), but you can combine multiple interface types in a macro.
This example shows how to define an interface-range macro named `enet_list` to select Fast Ethernet ports 1 to 4 and to verify the macro configuration:

```
Switch# configure terminal
Switch(config)# define interface-range enet_list fastethernet1/0/1 - 4
Switch(config)# end
Switch# show running-config | include define
define interface-range enet_list FastEthernet1/0/1 - 4
```

This example shows how to create a multiple-interface macro named `macro1`:

```
Switch# configure terminal
Switch(config)# define interface-range macro1 fastethernet1/0/1 - 2, fastethernet1/0/5 - 7
Switch(config)# end
```

This example shows how to enter interface range configuration mode for the interface-range macro `enet_list`:

```
Switch# configure terminal
Switch(config)# interface range macro enet_list
Switch(config-if-range)#
```

This example shows how to delete the interface-range macro `enet_list` and to verify that it was deleted.

```
Switch# configure terminal
Switch(config)# no define interface-range enet_list
Switch(config)# end
Switch# show run | include define
Switch#
```

## Configuring Ethernet Interfaces

These sections describe the default interface configuration and the optional features that you can configure on most physical interfaces:

- Default Ethernet Interface Configuration, page 9-11
- Configuring Interface Speed and Duplex Mode, page 9-12
- Configuring IEEE 802.3x Flow Control, page 9-14
- Configuring Auto-MDIX on a Port, page 9-15
- Adding a Description for an Interface, page 9-17

### Default Ethernet Interface Configuration

Table 9-1 shows the Ethernet interface default configuration, including some features that apply only to Layer 2 interfaces. For more details on the VLAN parameters listed in the table, see Chapter 11, “Configuring VLANS.” For details on controlling traffic to the port, see Chapter 24, “Configuring Port-Based Traffic Control.”

<table>
<thead>
<tr>
<th>Feature</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Ethernet Interface Configuration</td>
<td>Page 9-11</td>
</tr>
<tr>
<td>Configuring Interface Speed and Duplex Mode</td>
<td>Page 9-12</td>
</tr>
<tr>
<td>Configuring IEEE 802.3x Flow Control</td>
<td>Page 9-14</td>
</tr>
<tr>
<td>Configuring Auto-MDIX on a Port</td>
<td>Page 9-15</td>
</tr>
<tr>
<td>Adding a Description for an Interface</td>
<td>Page 9-17</td>
</tr>
</tbody>
</table>

**Note** To configure Layer 2 parameters, if the interface is in Layer 3 mode, you must enter the `switchport` interface configuration command without any parameters to put the interface into Layer 2 mode. This shuts down the interface and then re-enables it, which might generate messages on the device to which the interface is connected. Furthermore, when you use this command to put the interface into Layer 2 mode, you are deleting any Layer 3 characteristics configured on the interface.
Table 9-1  Default Layer 2 Ethernet Interface Configuration

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating mode</td>
<td>Layer 2 or switching mode (switchport command).</td>
</tr>
<tr>
<td>Allowed VLAN range</td>
<td>VLANs 1–4094.</td>
</tr>
<tr>
<td>Default VLAN (for access ports)</td>
<td>VLAN 1 (Layer 2 interfaces only).</td>
</tr>
<tr>
<td>Native VLAN (for 802.1Q trunks)</td>
<td>VLAN 1 (Layer 2 interfaces only).</td>
</tr>
<tr>
<td>VLAN trunking</td>
<td>Switchport mode dynamic auto (supports DTP) (Layer 2 interfaces only).</td>
</tr>
<tr>
<td>Port enable state</td>
<td>All ports are enabled.</td>
</tr>
<tr>
<td>Port description</td>
<td>None defined.</td>
</tr>
<tr>
<td>Speed</td>
<td>Autonegotiate.</td>
</tr>
<tr>
<td>Duplex mode</td>
<td>Autonegotiate.</td>
</tr>
<tr>
<td>Flow control</td>
<td>Flow control is set to receive: off. It is always off for sent packets.</td>
</tr>
<tr>
<td>EtherChannel (PAgP)</td>
<td>Disabled on all Ethernet ports. See Chapter 35, “Configuring EtherChannels and Link-State Tracking.”</td>
</tr>
<tr>
<td>Port blocking (unknown multicast and unknown unicast traffic)</td>
<td>Disabled (not blocked) (Layer 2 interfaces only). See the “Configuring Port Blocking” section on page 24-7.</td>
</tr>
<tr>
<td>Broadcast, multicast, and unicast storm control</td>
<td>Disabled. See the “Default Storm Control Configuration” section on page 24-3.</td>
</tr>
<tr>
<td>Protected port</td>
<td>Disabled (Layer 2 interfaces only). See the “Configuring Protected Ports” section on page 24-6.</td>
</tr>
<tr>
<td>Port security</td>
<td>Disabled (Layer 2 interfaces only). See the “Default Port Security Configuration” section on page 24-11. L2</td>
</tr>
<tr>
<td>Port Fast</td>
<td>Disabled.</td>
</tr>
</tbody>
</table>

Configuring Interface Speed and Duplex Mode

Ethernet interfaces on the switch operate at 10, 100, or 1000 Mb/s and in either full- or half-duplex mode. In full-duplex mode, two stations can send and receive traffic at the same time. Normally, 10-Mb/s ports operate in half-duplex mode, which means that stations can either receive or send traffic.

Switch models include combinations of Fast Ethernet (10/100-Mb/s) ports or Gigabit Ethernet SFP standard and ES module slots supporting Gigabit SFP modules.

These sections describe how to configure the interface speed and duplex mode:

- Speed and Duplex Configuration Guidelines, page 9-13
- Setting the Interface Speed and Duplex Parameters, page 9-13
### Speed and Duplex Configuration Guidelines

When configuring an interface speed and duplex mode, note these guidelines:

- If both ends of the line support autonegotiation, we highly recommend the default setting of **auto** negotiation.
- If one interface supports autonegotiation and the other end does not, configure duplex and speed on both interfaces; do not use the **auto** setting on the supported side.
- For 10/100 Mb/s ports, if both speed and duplex are set to specific values, the link operates at the negotiated speed and duplex value.
- You can configure interface speed on Fast Ethernet (10/100-Mb/s) ports. You can configure duplex mode to full, half, or autonegotiate on Fast Ethernet ports.
- You cannot configure duplex mode on SFP module ports unless a Cisco 1000BASE-T SFP module or a Cisco 100BASE-FX MMF SFP module is in the port. All other SFP modules operate only in full-duplex mode.
  - When a Cisco1000BASE-T SFP module is in the SFP module port, you can configure duplex mode to **auto** or **full**.
  - When a Cisco100BASE-FX SFP module is in the SFP module port, you can configure duplex mode to **half** or **full**. The ES ports do not support the 100BASE-FX SFP module. Although the **auto** keyword is available, it puts the interface into half-duplex mode (the default).
- You cannot configure speed on SFP module ports, except to **nonnegotiate**. However, when a 1000BASE-T SFP module is in the SFP module port, the speed can be configured to **10**, **100**, **1000**, or **auto**, but not **nonnegotiate**.

---

#### Caution

The ES ports do not support 10 or 100 Mb/s operation. Setting the speed on an ES port to 10 or 100 Mb/s, or to **auto** if the interface is connected to a 10/100 interface on another switch, can result in severe data loss if the interface is connected to a 10/100 interface on another switch.

- When STP is enabled and a port is reconfigured, the switch can take up to 30 seconds to check for loops. The port LED is amber while STP reconfigures.

#### Caution

Changing the interface speed and duplex mode configuration might shut down and re-enable the interface during the reconfiguration.

### Setting the Interface Speed and Duplex Parameters

Beginning in privileged EXEC mode, follow these steps to set the speed and duplex mode for a physical interface:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>interface interface-id</code></td>
<td>Enter interface configuration mode and the physical interface identification.</td>
</tr>
</tbody>
</table>
## Configuring Ethernet Interfaces

### Step 3

**Command**

```
speed {10 | 100 | 1000 | auto [10 | 100 | 1000] | nonegotiate}
```

**Purpose**

Enter the appropriate speed parameter for the port:

- Enter 10, 100, or 1000 to set a specific speed for the port. The 1000 keyword is not available on 10/100 Mb/s ports.
- Enter auto to enable the interface to autonegotiate speed with the device connected to the interface. If you use the 10, 100, or 1000 keywords with the auto keyword, the port only autonegotiates at the specified speeds.
- The nonegotiate keyword is available only for SFP module ports. SFP module ports operate only at 1000 Mb/s but can be configured to not negotiate if connected to a device that does not support autonegotiation.

For information about speed settings, see the “Speed and Duplex Configuration Guidelines” section on page 9-13.

### Step 4

**Command**

```
duplex {auto | full | half}
```

**Purpose**

Enter the duplex parameter for the interface.

Beginning with Cisco IOS Release 12.2(25)EXA, you can configure the duplex setting when the speed is set to auto.

For information about duplex settings, see the “Speed and Duplex Configuration Guidelines” section on page 9-13.

### Step 5

**Command**

```
end
```

**Purpose**

Return to privileged EXEC mode.

### Step 6

**Command**

```
show interfaces interface-id
```

**Purpose**

Display the interface speed and duplex mode configuration.

### Step 7

**Command**

```
copy running-config startup-config
```

(Optional) Save your entries in the configuration file.

---

**Use the no speed and no duplex interface configuration commands to return the interface to the default speed and duplex settings (autonegotiate). To return all interface settings to the defaults, use the default interface interface-id interface configuration command.**

This example shows how to set the speed to 10 Mb/s and the duplex mode to half on an port:

```
Switch# configure terminal
Switch(config)# interface fastethernet1/0/3
Switch(config-if)# speed 10
Switch(config-if)# duplex half
```

---

### Configuring IEEE 802.3x Flow Control

Flow control enables connected Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end. If one port experiences congestion and cannot receive any more traffic, it notifies the other port to stop sending until the condition clears by sending a pause frame. Upon receipt of a pause frame, the sending device stops sending any data packets, which prevents any loss of data packets during the congestion period.

**Note**

Catalyst 3750 Metro switch ports receive, but do not send pause frames.

You use the `flowcontrol` interface configuration command to set the interface’s ability to receive pause frames to on, off, or desired. The default state is off.
When set to desired, an interface can operate with an attached device that is required to send flow-control packets or with an attached device that is not required to but can send flow-control packets. These rules apply to flow control settings on the device:

- receive on (or desired): The port cannot send pause frames but can operate with an attached device that is required to or can send pause frames; the port can receive pause frames.
- receive off: Flow control does not operate in either direction. In case of congestion, no indication is given to the link partner, and no pause frames are sent or received by either device.

Note

For details on the command settings and the resulting flow control resolution on local and remote ports, see the flowcontrol interface configuration command in the command reference for this release.

Beginning in privileged EXEC mode, follow these steps to configure flow control on an interface:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>flowcontrol {receive} {on</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
</tr>
<tr>
<td>Step 5</td>
<td>show interfaces interface-id</td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To disable flow control, use the flowcontrol receive off interface configuration command.

This example shows how to turn on flow control on a port:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# flowcontrol receive on
Switch(config-if)# end
```

### Configuring Auto-MDIX on a Port

When automatic medium-dependent-interface crossover (Auto-MDIX) is enabled on an port, the port automatically detects the required cable connection type (straight through or crossover) and configures the connection appropriately. When connecting switches without the Auto-MDIX feature, you must use straight-through cables to connect to devices such as servers, workstations, or routers and crossover cables to connect to other switches or repeaters. With Auto-MDIX enabled, you can use either type of cable to connect to other devices, and the interface automatically corrects for any incorrect cabling. For more information about cabling requirements, see the hardware installation guide.

Auto-MDIX is enabled by default. When you enable Auto-MDIX, you must also set the speed and duplex on the port to auto so that for the feature to operate correctly. Auto-MDIX is supported on all 10/100 Mb/s ports and on 10/100/1000 BASE-T/TX SFP module ports. It is not supported on 1000 BASE-SX or -LX SFP module ports.
ES ports do not support 10 or 100 Mb/s operation. When a 1000BASE-T SFP module is inserted in an ES module port, if you set the speed to auto to enable Auto-MDIX, be sure that the interface is connected to a Gigabit interface. Setting the speed to auto can result in severe data loss if the interface is connected to a 10/100 interface on another switch.

Table 9-2 shows the link states that results from Auto-MDIX settings and correct and incorrect cabling.

### Table 9-2  Link Conditions and Auto-MDIX Settings

<table>
<thead>
<tr>
<th>Local Side Auto-MDIX</th>
<th>Remote Side Auto-MDIX</th>
<th>With Correct Cabling</th>
<th>With Incorrect Cabling</th>
</tr>
</thead>
<tbody>
<tr>
<td>On</td>
<td>On</td>
<td>Link up</td>
<td>Link up</td>
</tr>
<tr>
<td>On</td>
<td>Off</td>
<td>Link up</td>
<td>Link up</td>
</tr>
<tr>
<td>Off</td>
<td>On</td>
<td>Link up</td>
<td>Link up</td>
</tr>
<tr>
<td>Off</td>
<td>Off</td>
<td>Link up</td>
<td>Link down</td>
</tr>
</tbody>
</table>

Beginning in privileged EXEC mode, follow these steps to configure Auto-MDIX on a port:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enter global configuration mode</td>
</tr>
<tr>
<td><strong>Step 2</strong> interface interface-id</td>
<td>Enter interface configuration mode for the physical interface to be configured.</td>
</tr>
<tr>
<td><strong>Step 3</strong> speed auto</td>
<td>Configure the port to autonegotiate speed with the connected device.</td>
</tr>
<tr>
<td><strong>Step 4</strong> duplex auto</td>
<td>Configure the port to autonegotiate duplex mode with the connected device.</td>
</tr>
<tr>
<td><strong>Step 5</strong> mdix auto</td>
<td>Enable Auto-MDIX on the port.</td>
</tr>
<tr>
<td><strong>Step 6</strong> end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 7</strong> show controllers ethernet-controller interface-id phy</td>
<td>Verify the operational state of the Auto-MDIX feature on the interface.</td>
</tr>
<tr>
<td><strong>Step 8</strong> copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable Auto-MDIX, use the **no mdix auto** interface configuration command.

This example shows how to enable Auto-MDIX on a port:

```plaintext
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# speed auto
Switch(config-if)# duplex auto
Switch(config-if)# mdix auto
Switch(config-if)# end
```
Adding a Description for an Interface

You can add a description about an interface to help you remember its function. The description appears in the output of these privileged EXEC commands: `show configuration`, `show running-config`, and `show interfaces`.

Beginning in privileged EXEC mode, follow these steps to add a description for an interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>interface interface-id</td>
<td>Enter interface configuration mode, and enter the interface for which you are adding a description.</td>
</tr>
<tr>
<td>3</td>
<td>description string</td>
<td>Add a description (up to 240 characters) for an interface.</td>
</tr>
<tr>
<td>4</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>5</td>
<td>show interfaces interface-id description or show running-config</td>
<td>Verify your entry.</td>
</tr>
<tr>
<td>6</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Use the `no description` interface configuration command to delete the description.

This example shows how to add a description on a port and to verify the description:

```
Switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# description Connects to Marketing
Switch(config-if)# end
Switch# show interfaces gigabitethernet1/0/2 description
Interface Status         Protocol Description
Gi1/0/2 admin down     down     Connects to Marketing
```

Configuring Layer 3 Interfaces

The switch supports these types of Layer 3 interfaces:

- SVIs: You should configure SVIs for any VLANs for which you want to route traffic. SVIs are created when you enter a VLAN ID following the `interface vlan` global configuration command. To delete an SVI, use the `no interface vlan` global configuration command.

  **Note** When you create an SVI, it does not become active until it is associated with a physical port. For information about assigning Layer 2 ports to VLANs, see Chapter 11, “Configuring VLANs.”

- Routed ports: Routed ports are physical ports configured to be in Layer 3 mode by using the `no switchport` interface configuration command.
Layer 3 EtherChannel ports: EtherChannel interfaces made up of routed ports.

EtherChannel port interfaces are described in Chapter 35, “Configuring EtherChannels and Link-State Tracking.”

A Layer 3 switch can have an IP address assigned to each routed port and SVI.

There is no defined limit to the number of SVIs and routed ports that can be configured in a switch. However, the interrelationship between the number of SVIs and routed ports and the number of other features being configured might have an impact on CPU usage because of hardware limitations. If the switch is using maximum hardware resources, attempts to create a routed port or SVI have these results:

- If you try to create a new routed port, the switch generates a message that there are not enough resources to convert the interface to a routed port, and the interface remains as a switchport.
- If you try to create an extended-range VLAN, an error message is generated, and the extended-range VLAN is rejected.
- If the switch is notified by VLAN Trunking Protocol (VTP) of a new VLAN, it sends a message that there are not enough hardware resources available and shuts down the VLAN. The output of the show vlan user EXEC command shows the VLAN in a suspended state.
- If the switch attempts to boot up with a configuration that has more VLANs and routed ports than hardware can support, the VLANs are created, but the routed ports are shut down, and the switch sends a message that this was due to insufficient hardware resources.

All Layer 3 interfaces require an IP address to route traffic. This procedure shows how to configure an interface as a Layer 3 interface and how to assign an IP address to an interface.

**Note**

If the physical port is in Layer 2 mode (the default), you must enter the `no switchport` interface configuration command to put the interface into Layer 3 mode. Entering a `no switchport` command disables and then re-enables the interface, which might generate messages on the device to which the interface is connected.

Beginning in privileged EXEC mode, follow these steps to configure a Layer 3 interface:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface { {fastethernet</td>
</tr>
<tr>
<td>Step 3</td>
<td>no switchport</td>
</tr>
<tr>
<td>Step 4</td>
<td>ip address ip_address subnet_mask</td>
</tr>
<tr>
<td>Step 5</td>
<td>no shutdown</td>
</tr>
<tr>
<td>Step 6</td>
<td>end</td>
</tr>
<tr>
<td>Step 8</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To remove an IP address from an interface, use the `no ip address` interface configuration command.
This example shows how to configure a port as a routed port and to assign it an IP address:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# no switchport
Switch(config-if)# ip address 192.20.135.21 255.255.255.0
Switch(config-if)# no shutdown
```

### Configuring the System MTU

The default maximum transmission unit (MTU) size for frames received and transmitted on all interfaces on the switch is 1500 bytes. You can increase the MTU size for all interfaces operating at 10 or 100 Mb/s by using the `system mtu` global configuration command. You can increase the MTU size to support jumbo frames on all Gigabit Ethernet interfaces by using the `system mtu jumbo` global configuration command. Starting with Cisco IOS Release 12.2(55)SE, you can set an alternate MTU size to be applied so specific interfaces by using the `system mtu alternate` global configuration command. You can define only one alternate MTU size on the switch, but you can apply it to multiple interfaces.

**Note**

You cannot configure a routing MTU size that exceeds the system MTU size. If you change the system MTU size to a value smaller than the currently configured routing MTU size, the configuration change is accepted, but not applied until the next switch reset. When the configuration change takes effect, the routing MTU size automatically defaults to the new system MTU size.

Gigabit Ethernet ports MTU size is configured by the `system mtu jumbo` command. Fast Ethernet ports are not affected by this command because jumbo frames are not supported on 10/100 interfaces, including 100BASE-FX and 100BASE-BX SFP modules. If you do not configure the `system mtu jumbo` command, the setting of the `system mtu` command applies to all Gigabit Ethernet interfaces.

On an enhanced-services (ES) port you can use the `mpls mtu` interface configuration command to set the MTU size for multiprotocol label switching (MPLS) labeled packets. You can increase the size of MPLS labeled packets up to the size configured for jumbo packets. Because labeling a packet makes it larger, we recommend setting the system MTU and the MPLS MTU to the same value, to prevent dropping of labeled packets.

The switch supports a maximum MTU size for 10/100 interfaces of 1998 bytes. The maximum MTU size for Gigabit interfaces is 9000 bytes.

You cannot set the MTU size for an individual interface; you set it for all Fast Ethernet or all Gigabit Ethernet interfaces on the switch. When you change the MTU size, you must reset the switch before the new configuration takes effect. The `system mtu routing` command does not require a switch reset to take effect.

To define an alternate MTU size, enter the `system mtu alternate bytes` global configuration command. You then apply the alternate size to specified interfaces by using the `system mtu alternate interface interface-id` global configuration command. The range of the alternate MTU is between the configured `system mtu` and `system jumbo mtu` sizes (1500 to 9000 bytes). When you apply an alternate MTU size to an interface, frames received on the interface that are greater than the configured size are dropped. You can configure an alternate MTU size for Fast Ethernet or Gigabit Ethernet interfaces, but you cannot apply an alternate MTU size greater than 1998 bytes on a Fast Ethernet interface. The alternate MTU size has no effect on the routing MTU size.

When an alternate MTU size is applied to ES ports, packets are treated as expected (forwarded or dropped), but large packets are not tagged as giant frames. Accounting is not supported on ES ports.
When you configure an alternate MTU size, you must reload the switch before the configuration takes effect.

When you configure an alternate MTU size, you must reload the switch before the configuration takes effect.

Note

The system MTU setting is saved in the switch environmental variable in NVRAM and becomes effective when the switch reloads. Unlike the system MTU routing configuration, the MTU settings you enter with the `system mtu` and `system mtu jumbo` commands are not saved in the switch configuration file, even if you enter the `copy running-config startup-config` privileged EXEC command. Therefore, if you use TFTP to configure a new switch by using a backup configuration file and want the system MTU to be other than the default, you must explicitly configure the `system mtu` and `system mtu jumbo` settings on the new switch and then reload the switch.

The size of frames that can be received by the switch CPU is limited to 1998 bytes, no matter what value was entered with the `system mtu` or `system mtu jumbo` commands. Although frames that are forwarded or routed typically are not received by the CPU, in some cases packets are sent to the CPU, such as traffic sent to control traffic, SNMP, or Telnet, or routing protocols.

Routed packets are subjected to MTU checks on the egress ports. The MTU value used for routed ports is derived from the `system mtu` configured value (not the `system mtu jumbo` value). That is, the routed MTU is never greater than the system MTU for any VLAN. The system MTU value is used by routing protocols when negotiating adjacencies and the MTU of the link. For example Open Shortest Path First (OSPF) protocol uses this MTU value before setting up an adjacency with a peer router. To view the MTU value for routed packets for a specific VLAN, use the `show platform port-asic mvrid` privileged EXEC command.

Routed packets are subjected to MTU checks on the egress ports. The MTU value used for routed ports is derived from the `system mtu` configured value (not the `system mtu jumbo` value). That is, the routed MTU is never greater than the system MTU for any VLAN. The system MTU value is used by routing protocols when negotiating adjacencies and the MTU of the link. For example Open Shortest Path First (OSPF) protocol uses this MTU value before setting up an adjacency with a peer router. To view the MTU value for routed packets for a specific VLAN, use the `show platform port-asic mvrid` privileged EXEC command.

Note

If Layer 2 Gigabit Ethernet interfaces are configured to accept frames greater than the 10/100 interfaces, jumbo frames ingressing on a Layer 2 Gigabit Ethernet interface and egressing on a Layer 2 10/100 interface are dropped.

Beginning in privileged EXEC mode, follow these steps to change the MTU size for all 10/100 or Gigabit Ethernet interfaces and to set an alternate MTU size for specified interfaces:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 system mtu bytes</td>
<td>(Optional) Change the MTU size for all interfaces on the switch that are operating at 10 or 100 Mb/s. The range is 1500 to 1998 bytes. The default is 1500 bytes.</td>
</tr>
<tr>
<td>Step 3 system mtu jumbo bytes</td>
<td>(Optional) Change the MTU size for all Gigabit Ethernet interfaces on the switch. The range is 1500 to 9000 bytes. The default is 1500 bytes.</td>
</tr>
</tbody>
</table>
## Configuring the System MTU

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td><code>system mtu alternate bytes</code></td>
<td>(Optional) Set an alternate MTU size. The range is between the configured system MTU size and the configured jumbo MTU size (1500 to 9000 bytes). The default is 1500 bytes.</td>
</tr>
<tr>
<td>5</td>
<td>`system mtu alternate interface {interface-id</td>
<td>range interface-range}`</td>
</tr>
<tr>
<td>6</td>
<td><code>system mtu routing bytes</code></td>
<td>(Optional) Change the system MTU for routed ports. The range is 1500 to the system MTU value. This is the maximum MTU that can be routed for all ports. Although larger packets can be accepted, they cannot be routed.</td>
</tr>
<tr>
<td>7</td>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>8</td>
<td><code>reload</code></td>
<td>Reload the operating system.</td>
</tr>
</tbody>
</table>

If you enter a value that is outside the allowed range for the specific type of interface, the value is not accepted.

Once the switch reloads, you can verify your settings by entering the `show system mtu` privileged EXEC command. To verify the MTU setting on an interface, enter the `show interface interface-id mtu`.

This example shows how to set the maximum packet size for Gigabit Ethernet interfaces to 1800 bytes:

```console
Switch(config)# system mtu jumbo 1800
Switch(config)# exit
Switch# reload
```

This example shows the response when you try to set Gigabit Ethernet interfaces to an out-of-range number:

```console
Switch(config)# system mtu jumbo 10000
^[% Invalid input detected at '^' marker.
```

This example shows how to set the maximum packet size for Gigabit Ethernet ports to 1800 bytes, to define an alternate MTU size of 1700 bytes and apply it to Gigabit Ethernet port 0/8. Changes are not applied until you reload the switch:

```console
Switch(config)# system mtu jumbo 1800
Switch(config)# system mtu alternate 1700
Changes to the Alternate MTU will not take effect until the next reload is done
Switch(config)# system mtu alternate interface gigabitethernet 0/0/8
Changes to the Alternate MTU on interface will not take effect until the next reload is done
Switch(config)# exit
Switch# reload
```

This example shows how to apply the alternate MTU to Gigabit Ethernet interfaces 1 to 10. Changes are not applied until you reload the switch:

```console
Switch(config)# system mtu alternate interface range gigabitethernet 1/0/1-10
Changes to the Alternate MTU on interface(s) will not take effect until the next reload is done
Switch(config)# exit
```
Monitoring and Maintaining the Interfaces

- Monitoring Interface Status, page 9-22
- Clearing and Resetting Interfaces and Counters, page 9-23
- Shutting Down and Restarting the Interface, page 9-23

Monitoring Interface Status

Commands entered at the privileged EXEC prompt display information about the interface, including the versions of the software and the hardware, the configuration, and statistics about the interfaces. Table 9-3 lists some of these interface monitoring commands. (You can display the full list of show commands by using the show ? command at the privileged EXEC prompt.) These commands are fully described in the Cisco IOS Interface Command Reference for Release 12.2.

Table 9-3  Show Commands for Interfaces

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show interfaces [interface-id]</td>
<td>Display the status and configuration of all interfaces or a specific interface.</td>
</tr>
<tr>
<td>show interfaces interface-id status [err-disabled]</td>
<td>Display interface status or a list of interfaces in an error-disabled state.</td>
</tr>
<tr>
<td>show interfaces [interface-id] mtu</td>
<td>Display the MTU setting on an interface.</td>
</tr>
<tr>
<td>show interfaces [interface-id] switchport</td>
<td>Display administrative and operational status of switching (nonrouting) ports. You can use this command to determine if a port is in routing or switching mode.</td>
</tr>
<tr>
<td>show interfaces [interface-id] description</td>
<td>Display the description configured on an interface or all interfaces and the interface status.</td>
</tr>
<tr>
<td>show interfaces [interface-id] transceiver [detail</td>
<td>dom-supported-list</td>
</tr>
<tr>
<td></td>
<td>- interface-id—(Optional) Display configuration and status for a specified physical interface.</td>
</tr>
<tr>
<td></td>
<td>- detail—(Optional) Display calibration properties, including high and low numbers and any alarm information for any Digital Optical Monitoring (DoM)-capable transceiver if one is installed in the switch.</td>
</tr>
<tr>
<td></td>
<td>- dom-supported-list—(Optional) List all supported DoM transceivers.</td>
</tr>
<tr>
<td></td>
<td>- module number—(Optional) Limit display to interfaces on module on the switch. The range is 1 to 9. This option is not available if you entered a specific interface ID.</td>
</tr>
<tr>
<td></td>
<td>- properties—(Optional) Display speed, duplex, and inline power settings on an interface</td>
</tr>
<tr>
<td></td>
<td>- threshold-table—(Optional) Display alarm and warning threshold table</td>
</tr>
<tr>
<td>show ip interface [interface-id]</td>
<td>Display the usability status of all interfaces configured for IP routing or the specified interface.</td>
</tr>
<tr>
<td>show running-config interface [interface-id]</td>
<td>Display the running configuration in RAM for the interface.</td>
</tr>
</tbody>
</table>
Table 9-3  Show Commands for Interfaces (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show version</td>
<td>Display the hardware configuration, software version, the names and sources of configuration files, and the boot images.</td>
</tr>
<tr>
<td>show controllers ethernet-controller interface-id phy</td>
<td>Verify the operational state of the Auto-MDIX feature on the interface.</td>
</tr>
</tbody>
</table>

Clearing and Resetting Interfaces and Counters

Table 9-4 lists the privileged EXEC mode clear commands that you can use to clear counters and reset interfaces.

Table 9-4  Clear Commands for Interfaces

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear counters [interface-id]</td>
<td>Clear interface counters.</td>
</tr>
<tr>
<td>clear interface interface-id</td>
<td>Reset the hardware logic on an interface.</td>
</tr>
<tr>
<td>clear line [number</td>
<td>console 0</td>
</tr>
</tbody>
</table>

To clear the interface counters shown by the show interfaces privileged EXEC command, use the clear counters privileged EXEC command. The clear counters command clears all current interface counters from the interface unless optional arguments are specified to clear only a specific interface type from a specific interface number.

Note

The clear counters privileged EXEC command does not clear counters retrieved by using Simple Network Management Protocol (SNMP), but only those seen with the show interface privileged EXEC command.

Shutting Down and Restarting the Interface

Shutting down an interface disables all functions on the specified interface and marks the interface as unavailable on all monitoring command displays. This information is communicated to other network servers through all dynamic routing protocols. The interface is not mentioned in any routing updates.

Beginning in privileged EXEC mode, follow these steps to shut down an interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>interface [vlan vlan-id]</td>
<td>Select the interface to be configured.</td>
</tr>
<tr>
<td></td>
<td>fastethernet</td>
<td>interface-id</td>
</tr>
<tr>
<td>3</td>
<td>shutdown</td>
<td>Shut down an interface.</td>
</tr>
<tr>
<td>4</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>5</td>
<td>show running-config</td>
<td>Verify your entry.</td>
</tr>
</tbody>
</table>
Use the **no shutdown** interface configuration command to restart the interface.

To verify that an interface is disabled, enter the **show interfaces** privileged EXEC command. A disabled interface is shown as *administratively down* in the **show interface** command display.
Configuring Smartports Macros

This chapter describes how to configure and apply Smartports macros on the Catalyst 3750 Metro switch.

For complete syntax and usage information for the commands used in this chapter, see the command reference for this release.

This chapter consists of these sections:

- Understanding Smartports Macros, page 10-1
- Configuring Smartports Macros, page 10-2
- Displaying Smartports Macros, page 10-8

Understanding Smartports Macros

Smartports macros provide a convenient way to save and share common configurations. You can use Smartports macros to enable features and settings based on the location of a switch in the network and for mass configuration deployments across the network.

Each Smartports macro is a set of command-line interface (CLI) commands that you define. Smartports macros do not contain new CLI commands; they are simply a group of existing CLI commands.

When you apply a Smartports macro on an interface, the CLI commands within the macro are configured on the interface. When the macro is applied to an interface, the existing interface configurations are not lost. The new commands are added to the interface and are saved in the running configuration file.

There are Cisco-default Smartports macros embedded in the switch software (see Table 10-1). You can display these macros and the commands they contain by using the show parser macro user EXEC command.

<table>
<thead>
<tr>
<th>Macro Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cisco-global</td>
<td>Use this global configuration macro to enable rapid PVST+, loop guard, and dynamic port error recovery for link state failures.</td>
</tr>
<tr>
<td>cisco-desktop</td>
<td>Use this interface configuration macro for increased network security and reliability when connecting a desktop device, such as a PC, to a switch port.</td>
</tr>
</tbody>
</table>
Configuring Smartports Macros

You can create a new Smartports macro or use an existing macro as a template to create a new macro that is specific to your application. After you create the macro, you can apply it globally to a switch or to a switch interface or range of interfaces.

This section includes information about:
- Default Smartports Macro Configuration, page 10-2
- Smartports Macro Configuration Guidelines, page 10-2
- Creating Smartports Macros, page 10-4
- Applying Smartports Macros, page 10-5
- Applying Cisco-Default Smartports Macros, page 10-6

### Default Smartports Macro Configuration

There are no Smartports macros enabled.

### Smartports Macro Configuration Guidelines

Follow these guidelines when configuring macros on your switch:

- When creating a macro, do not use the exit or end commands or change the command mode by using interface interface-id. This could cause commands that follow exit, end, or interface interface-id to execute in a different command mode.
- When creating a macro, all CLI commands should be in the same configuration mode.

---

**Table 10-1  Cisco-Default Smartports Macros (continued)**

<table>
<thead>
<tr>
<th>Macro Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cisco-phone</td>
<td>Use this interface configuration macro when connecting a desktop device such as a PC with a Cisco IP Phone to a switch port. This macro is an extension of the cisco-desktop macro and provides the same security and resiliency features, but with the addition of dedicated voice VLANs to ensure proper treatment of delay-sensitive voice traffic.</td>
</tr>
<tr>
<td>cisco-switch</td>
<td>Use this interface configuration macro when connecting an access switch and a distribution switch or between access switches connected using GigaStack modules or GBICs.</td>
</tr>
<tr>
<td>cisco-router</td>
<td>Use this interface configuration macro when connecting the switch and a WAN router.</td>
</tr>
<tr>
<td>cisco-wireless</td>
<td>Use this interface configuration macro when connecting the switch and a wireless access point.</td>
</tr>
</tbody>
</table>

1. Cisco-default Smartports macros vary depending on the software version running on your switch.
• When creating a macro that requires the assignment of unique values, use the parameter value keywords to designate values specific to the interface. Keyword matching is case sensitive. All matching occurrences of the keyword are replaced with the corresponding value. Any full match of a keyword, even if it is part of a larger string, is considered a match and is replaced by the corresponding value.

• Macro names are case sensitive. For example, the commands macro name Sample-Macro and macro name sample-macro will result in two separate macros.

• Some macros might contain keywords that require a parameter value. You can use the macro global apply macro-name ? global configuration command or the macro apply macro-name ? interface configuration command to display a list of any required values in the macro. If you apply a macro without entering the keyword values, the commands are invalid and are not applied.

• When a macro is applied globally to a switch or to a switch interface, all existing configuration on the interface is retained. This is helpful when applying an incremental configuration.

• If you modify a macro definition by adding or deleting commands, the changes are not reflected on the interface where the original macro was applied. You need to reapply the updated macro on the interface to apply the new or changed commands.

• You can use the macro global trace macro-name global configuration command or the macro trace macro-name interface configuration command to apply and debug a macro to find any syntax or configuration errors. If a command fails because of a syntax error or a configuration error, the macro continues to apply the remaining commands.

• Some CLI commands are specific to certain interface types. If a macro is applied to an interface that does not accept the configuration, the macro will fail the syntax check or the configuration check, and the switch will return an error message.

• Applying a macro to an interface range is the same as applying a macro to a single interface. When you use an interface range, the macro is applied sequentially to each interface within the range. If a macro command fails on one interface, it is still applied to the remaining interfaces.

• When you apply a macro to a switch or a switch interface, the macro name is automatically added to the switch or interface. You can display the applied commands and macro names by using the show running-config user EXEC command.

There are Cisco-default Smartports macros embedded in the switch software (see Table 10-1). You can display these macros and the commands they contain by using the show parser macro user EXEC command.

Follow these guidelines when you apply a Cisco-default Smartports macro on an interface:

• Display all macros on the switch by using the show parser macro user EXEC command. Display the contents of a specific macro by using the show parser macro macro-name user EXEC command.

• Keywords that begin with $ mean that a unique parameter value is required. Append the Cisco-default macro with the required values by using the parameter value keywords. The Cisco-default macros use the $ character to help identify required keywords. There is no restriction on using the $ character to define keywords when you create a macro.
Creating Smartports Macros

Beginning in privileged EXEC mode, follow these steps to create a Smartports macro:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>macro name macro-name</td>
<td>Create a macro definition, and enter a macro name. A macro definition can contain up to 3000 characters. Enter the macro commands with one command per line. Use the @ character to end the macro. Use the # character at the beginning of a line to enter comment text within the macro. (Optional) You can define keywords within a macro by using a help string to specify the keywords. Enter # macro keywords word to define the keywords that are available for use with the macro. Separated by a space, you can enter up to three help string keywords in a macro. Macro names are case sensitive. For example, the commands macro name Sample-Macro and macro name sample-macro will result in two separate macros. We recommend that you do not use the exit or end commands or change the command mode by using interface interface-id in a macro. This could cause any commands following exit, end, or interface interface-id to execute in a different command mode. For best results, all commands in a macro should be in the same configuration mode.</td>
</tr>
<tr>
<td>3</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>4</td>
<td>show parser macro name macro-name</td>
<td>Verify that the macro was created.</td>
</tr>
</tbody>
</table>

The no form of the macro name global configuration command only deletes the macro definition. It does not affect the configuration of those interfaces on which the macro is already applied.

This example shows how to create a macro that defines the switchport access VLAN and the number of secure MAC addresses and also includes two help string keywords by using # macro keywords:

```
Switch(config)# macro name test
switchport access vlan $VLANID
switchport port-security maximum $MAX
#macro keywords $VLANID $MAX
@
```
Applying Smartports Macros

Beginning in privileged EXEC mode, follow these steps to apply a Smartports macro:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>configure terminal</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
</tbody>
</table>

| Step 2          | **macro global (apply | trace)**                                    | Purpose                                                                 |
|-----------------|-------------------------------------------------|-------------------------------------------------------------------------|
|                 | **macro-name [parameter {value}]**              | Apply each individual command defined in the macro to the switch by     |
|                 |                                                 | entering **macro global apply macro-name**. Specify **macro global trace** | |
|                 |                                                 | **macro-name** to apply and debug a macro to find any syntax or         |
|                 |                                                 | configuration errors.                                                   |
|                 |                                                 | (Optional) Specify unique parameter values that are specific to the     |
|                 |                                                 | switch. You can enter up to three keyword-value pairs. Parameter        |
|                 |                                                 | keyword matching is case sensitive. All matching occurrences of the     |
|                 |                                                 | keyword are replaced with the corresponding value.                     |
|                 |                                                 | Some macros might contain keywords that require a parameter value.     |
|                 |                                                 | You can use the **macro global apply macro-name ?** command to display  |
|                 |                                                 | a list of any required values in the macro. If you apply a macro without |
|                 |                                                 | entering the keyword values, the commands are invalid and are not       |
|                 |                                                 | applied.                                                               |

| Step 3          | **macro global description text**               | (Optional) Enter a description about the macro that is applied to the    |
|-----------------|-------------------------------------------------| switch.                                                                |

| Step 4          | **interface interface-id**                      | (Optional) Enter interface configuration mode, and specify the interface |
|-----------------|-------------------------------------------------| on which to apply the macro.                                           |

| Step 5          | **default interface interface-id**              | (Optional) Clear all configuration from the specified interface.        |

| Step 6          | **macro (apply | trace) macro-name**                   | Purpose                                                                 |
|-----------------|---------------------------------------------|-------------------------------------------------------------------------|
|                 | **parameter {value}]**                      | Apply each individual command defined in the macro to the interface by  |
|                 | **parameter {value}]**                      | entering **macro apply macro-name**. Specify **macro trace macro-name** |
|                 | **parameter {value}]**                      | to apply and debug a macro to find any syntax or configuration errors.  |
|                 |                                             | (Optional) Specify unique parameter values that are specific to the     |
|                 |                                             | interface. You can enter up to three keyword-value pairs. Parameter     |
|                 |                                             | keyword matching is case sensitive. All matching occurrences of the     |
|                 |                                             | keyword are replaced with the corresponding value.                     |
|                 |                                             | Some macros might contain keywords that require a parameter value.     |
|                 |                                             | You can use the **macro apply macro-name ?** command to display a list  |
|                 |                                             | of any required values in the macro. If you apply a macro without       |
|                 |                                             | entering the keyword values, the commands are invalid and are not       |
|                 |                                             | applied.                                                               |

| Step 7          | **macro description text**                    | (Optional) Enter a description about the macro that is applied to the    |
|-----------------|------------------------------------------------| interface.                                                            |

| Step 8          | **end**                                       | Return to privileged EXEC mode.                                        |

| Step 9          | **show parser macro description [interface interface-id]** | Verify that the macro is applied to the interface.                      |

| Step 10         | **copy running-config startup-config**        | (Optional) Save your entries in the configuration file.                |

You can delete a global macro-applied configuration on a switch only by entering the **no** version of each command that is in the macro. You can delete a macro-applied configuration on an interface by entering the **default interface interface-id** interface configuration command.
This example shows how to apply the user-created macro called `snmp`, to set the hostname address to `test-server`, and to set the IP precedence value to **7**:

```
Switch(config)# macro global apply snmp ADDRESS test-server VALUE 7
```

This example shows how to debug the user-created macro called `snmp` by using the `macro global trace` global configuration command to find any syntax or configuration errors in the macro when it is applied to the switch.

```
Switch(config)# macro global trace snmp VALUE 7
Applying command...'snmp-server enable traps port-security'
Applying command...'snmp-server enable traps linkup'
Applying command...'snmp-server enable traps linkdown'
Applying command...'snmp-server host'
%Error Unknown error.
Applying command...'snmp-server ip precedence 7'
```

This example shows how to apply the user-created macro called `desktop-config` and to verify the configuration.

```
Switch(config)# interface fastethernet1/0/2
Switch(config-if)# macro apply desktop-config
Switch(config-if)# end
Switch# show parser macro description
<table>
<thead>
<tr>
<th>Interface</th>
<th>Macro Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa1/0/2</td>
<td>desktop-config</td>
</tr>
</tbody>
</table>
```

This example shows how to apply the user-created macro called `desktop-config` and to replace all occurrences of VLAN 1 with VLAN 25:

```
Switch(config-if)# macro apply desktop-config vlan 25
```

### Applying Cisco-Default Smartports Macros

Beginning in privileged EXEC mode, follow these steps to apply a Smartports macro:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>show parser macro</td>
</tr>
<tr>
<td>Step 2</td>
<td>show parser macro <code>macro-name</code></td>
</tr>
<tr>
<td>Step 3</td>
<td>configure terminal <code>macro-name</code></td>
</tr>
</tbody>
</table>
| Step 4  | `macro global {apply | trace} [macro-name | Append the Cisco-default macro with the required values by using the `parameter value` keywords and apply the macro to the switch. Keywords that begin with `$` mean that a unique parameter value is required.

You can use the `macro global apply macro-name ?` command to display a list of any required values in the macro. If you apply a macro without entering the keyword values, the commands are invalid and are not applied.

| Step 5  | `interface interface-id` | (Optional) Enter interface configuration mode, and specify the interface on which to apply the macro. |
| Step 6  | `default interface interface-id` | (Optional) Clear all configuration from the specified interface. |
### Chapter 10      Configuring Smartports Macros

**Step 7**

```bash
macro {apply | trace} macro-name
[parameter {value}] [parameter {value}] [parameter {value}]
```

Append the Cisco-default macro with the required values by using the `parameter value` keywords, and apply the macro to the interface. Keywords that begin with `$` mean that a unique parameter value is required.

You can use the `macro apply macro-name ?` command to display a list of any required values in the macro. If you apply a macro without entering the keyword values, the commands are invalid and are not applied.

**Step 8**

```
end
```

Return to privileged EXEC mode.

**Step 9**

```
show running-config interface interface-id
```

Verify that the macro is applied to an interface.

**Step 10**

```
copy running-config startup-config
```

(Optional) Save your entries in the configuration file.

---

You can delete a global macro-applied configuration on a switch only by entering the `no` version of each command that is in the macro. You can delete a macro-applied configuration on an interface by entering the `default interface interface-id` interface configuration command.

This example shows how to display the `cisco-desktop` macro, how to apply the macro, and to set the access VLAN ID to 25 on an interface:

```bash
Switch# show parser macro cisco-desktop
--------------------------------------------------------------
Macro name : cisco-desktop
Macro type : default
# Basic interface - Enable data VLAN only
# Recommended value for access vlan (AVID) should not be 1
switchport access vlan $AVID
switchport mode access

# Enable port security limiting port to a single
# MAC address -- that of desktop
switchport port-security
switchport port-security maximum 1

# Ensure port-security age is greater than one minute
# and use inactivity timer
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity

# Configure port as an edge network port
spanning-tree portfast
spanning-tree bpduguard enable
--------------------------------------------------------------
Switch#
Switch# configure terminal
Switch(config)# fastethernet1/0/4
Switch(config-if)# macro apply cisco-desktop $AVID 25
```
Displaying Smartports Macros

To display the Smartports macros, use one or more of the privileged EXEC commands in Table 10-2.

Table 10-2  Commands for Displaying Smartports Macros

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show parser macro</td>
<td>Displays all configured macros.</td>
</tr>
<tr>
<td>show parser macro name (macro-name)</td>
<td>Displays a specific macro.</td>
</tr>
<tr>
<td>show parser macro brief</td>
<td>Displays the configured macro names.</td>
</tr>
<tr>
<td>show parser macro description [interface (interface-id)]</td>
<td>Displays the macro description for all interfaces or for a specified interface.</td>
</tr>
</tbody>
</table>
Configuring VLANs

This chapter describes how to configure normal-range VLANs (VLAN IDs 1 to 1005) and extended-range VLANs (VLAN IDs 1006 to 4094) on the Catalyst 3750 Metro switch. It includes information about VLAN membership modes, VLAN configuration modes, VLAN trunks, and dynamic VLAN assignment from a VLAN Membership Policy Server (VMPS).

For complete syntax and usage information for the commands used in this chapter, see the command reference for this release.

The chapter includes these sections:

- Understanding VLANs, page 11-1
- Configuring Normal-Range VLANs, page 11-4
- Configuring Extended-Range VLANs, page 11-11
- Displaying VLANs, page 11-14
- Configuring VLAN Trunks, page 11-15
- Configuring VMPS, page 11-27

Understanding VLANs

A VLAN is a switched network that is logically segmented by function, project team, or application, without regard to the physical locations of the users. VLANs have the same attributes as physical LANs, but you can group end stations even if they are not physically located on the same LAN segment. Any switch port can belong to a VLAN, and unicast, broadcast, and multicast packets are forwarded and flooded only to end 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 a switch supporting fallback bridging, as shown in Figure 11-1. Because a VLAN is considered a separate logical network, it contains its own bridge MIB information and can support its own implementation of spanning tree. See Chapter 16, “Configuring STP.”

Before you create VLANs, you must decide whether to use VLAN Trunking Protocol (VTP) to maintain global VLAN configuration for your network. For more information on VTP, see Chapter 12, “Configuring VTP.”
Figure 11-1 shows an example of VLANs segmented into logically defined networks.

VLANs are often associated with IP subnetworks. For example, all the end stations in a particular IP subnet belong to the same VLAN. Interface VLAN membership on the switch is assigned manually on an interface-by-interface basis. When you assign switch interfaces to VLANs by using this method, it is known as interface-based, or static, VLAN membership.

Traffic between VLANs must be routed or fallback bridged. The switch can route traffic between VLANs by using switch virtual interfaces (SVIs). An SVI must be explicitly configured and assigned an IP address to route traffic between VLANs. For more information, see the “Switch Virtual Interfaces” section on page 9-4 and the “Configuring Layer 3 Interfaces” section on page 9-17.

If you plan to configure many VLANs on the switch and to not enable routing, you can use the `sdm prefer vlan` global configuration command to set the Switch Database Management (SDM) feature to the VLAN template, which configures system resources to support the maximum number of unicast MAC addresses. For more information on the SDM templates, see Chapter 6, “Configuring SDM Templates,” or see the `sdm prefer` command in the command reference for this release.

### Supported VLANs

The switch supports 1005 VLANs in VTP client, server, and transparent modes. VLANs are identified with a number from 1 to 4094. VLAN IDs 1002 through 1005 are reserved for Token Ring and FDDI VLANs. VTP only learns normal-range VLANs, with VLAN IDs 1 to 1005; VLAN IDs greater than 1005 are extended-range VLANs and are not stored in the VLAN database. The switch must be in VTP transparent mode when you create VLAN IDs from 1006 to 4094.
Although the switch supports a total of 1005 (normal-range and extended-range) VLANs, the number of routed ports, SVIs, and other configured features affects the use of the switch hardware.

The switch supports per-VLAN spanning-tree plus (PVST+) or rapid PVST+ with a maximum of 128 spanning-tree instances. One spanning-tree instance is allowed per VLAN. See the “Normal-Range VLAN Configuration Guidelines” section on page 11-6 for more information about the number of spanning-tree instances and the number of VLANs. The switch supports both Inter-Switch Link (ISL) and IEEE 802.1Q trunking methods for sending VLAN traffic over 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 to which it can belong. Table 11-1 lists the membership modes and membership and VTP characteristics.

<table>
<thead>
<tr>
<th>Membership Mode</th>
<th>VLAN Membership Characteristics</th>
<th>VTP Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static-access</td>
<td>A static-access port can belong to one VLAN and is manually assigned to that VLAN. For more information, see the “Assigning Static-Access Ports to a VLAN” section on page 11-10.</td>
<td>VTP is not required. If you do not want VTP to globally propagate information, set the VTP mode to transparent to disable VTP. To participate in VTP, there must be at least one trunk port on the switch connected to a trunk port of a second switch.</td>
</tr>
<tr>
<td>Trunk (ISL or IEEE 802.1Q)</td>
<td>A trunk port is a member of all VLANs by default, including extended-range VLANs, but membership can be limited by configuring the allowed-VLAN list. You can also modify the pruning-eligible list to block flooded traffic to VLANs on trunk ports that are included in the list. For information about configuring trunk ports, see the “Configuring an Ethernet Interface as a Trunk Port” section on page 11-19.</td>
<td>VTP is recommended but not required. 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.</td>
</tr>
<tr>
<td>Dynamic access</td>
<td>A dynamic-access port can belong to one VLAN (VLAN ID 1 to 4094) and is dynamically assigned by a VMPS. The VMPS can be a Catalyst 5000 or Catalyst 6500 series switch, for example, but never a Catalyst 3750 Metro switch. The Catalyst 3750 Metro switch is a VMPS client. You can have dynamic-access ports and trunk ports on the same switch, but you must connect the dynamic-access port to an end station or hub and not to another switch. For configuration information, see the “Configuring Dynamic-Access Ports on VMPS Clients” section on page 11-30.</td>
<td>VTP is required. Configure the VMPS and the client with the same VTP domain name. To participate in VTP, there must be at least one trunk port on the switch connected to a trunk port of a second switch.</td>
</tr>
</tbody>
</table>

Note: Beginning with Cisco IOS Release 12.2(22)EY, ISL trunking is not supported on enhanced-services (ES) ports. ES ports support only IEEE 802.1Q encapsulation.
Configuring Normal-Range VLANs

Normal-range VLANs are VLANs with VLAN IDs 1 to 1005. If the switch is in VTP server or transparent mode, you can add, modify or remove configurations for VLANs 2 to 1001 in the VLAN database. (VLAN IDs 1 and 1002 to 1005 are automatically created and cannot be removed.)

When the switch is in VTP transparent mode, you can also create extended-range VLANs (VLANs with IDs from 1006 to 4094), but these VLANs are not saved in the VLAN database. See the “Configuring Extended-Range VLANs” section on page 11-11.

Table 11-1 Port Membership Modes (continued)

<table>
<thead>
<tr>
<th>Membership Mode</th>
<th>VLAN Membership Characteristics</th>
<th>VTP Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private VLAN</td>
<td>A private VLAN port is a host or promiscuous port that belongs to a private VLAN primary or secondary VLAN. To use this feature, the switch must be running the enhanced multilayer image (EMI). For information about private VLANs, see Chapter 13, “Configuring Private VLANs.”</td>
<td>The switch must be in VTP transparent mode when you configure private VLANs. When private VLANs are configured on the switch, do not change VTP mode from transparent to client or server mode.</td>
</tr>
<tr>
<td>Voice VLAN</td>
<td>A voice VLAN port is an access port attached to a Cisco IP Phone, configured to use one VLAN for voice traffic and another VLAN for data traffic from a device attached to the phone. For more information about voice VLAN ports, see Chapter 14, “Configuring Voice VLAN.”</td>
<td>VTP is not required; it has no effect on voice VLAN.</td>
</tr>
<tr>
<td>Tunnel (dot1q-tunnel)</td>
<td>Tunnel ports are used for IEEE 802.1Q tunneling to maintain customer VLAN integrity across a service provider network. You configure a tunnel port on an edge switch in the service provider network and connect it to an IEEE 802.1Q trunk port on a customer interface, creating an asymmetric link. A tunnel port belongs to a single VLAN that is dedicated to tunneling. For more information about tunnel ports, see Chapter 15, “Configuring IEEE 802.1Q and Layer 2 Protocol Tunneling.”</td>
<td>VTP is not required. You manually assign the tunnel port to a VLAN by using the switchport access vlan interface configuration command.</td>
</tr>
</tbody>
</table>

For more detailed definitions of the modes and their functions, see Table 11-4 on page 11-16.

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 Table” section on page 5-19.
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, use the commands described in these sections and in the command reference for this release. To change the VTP configuration, see Chapter 12, “Configuring VTP.”

You use the interface configuration mode to define the port membership mode and to add and remove ports from VLANs. The results of these commands are written to the running-configuration file, and you can display the file by entering the show running-config privileged EXEC command.

You can set these parameters when you create a new normal-range VLAN or modify an existing VLAN in the VLAN 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

This section does not provide configuration details for most of these parameters. For complete information on the commands and parameters that control VLAN configuration, see the command reference for this release.

This section includes information about these topics about normal-range VLANs:

- Token Ring VLANs, page 11-6
- Normal-Range VLAN Configuration Guidelines, page 11-6
- Saving VLAN Configuration, page 11-7
- Default Ethernet VLAN Configuration, page 11-7
- Creating or Modifying an Ethernet VLAN, page 11-8
- Deleting a VLAN, page 11-9
- Assigning Static-Access Ports to a VLAN, page 11-10
Chapter 11  Configuring VLANs

Token Ring VLANs

Although the switch does 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 VTP Version 2 advertise information about these Token Ring VLANs:

- Token Ring TrBRF VLANs
- Token Ring TrCRF VLANs

For more information on configuring Token Ring VLANs, see the Catalyst 5000 Series Software Configuration Guide.

Normal-Range VLAN Configuration Guidelines

Follow these guidelines when creating and modifying normal-range VLANs in your network:

- The switch supports 1005 VLANs in VTP client, server, and transparent modes.
- Normal-range VLANs are identified with a number between 1 and 1001. VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs.
- VLAN configuration for VLANs 1 to 1005 are always saved in the VLAN database. If VTP mode is transparent, VTP and VLAN configuration is also saved in the switch running configuration file.
- The switch also supports VLAN IDs 1006 through 4094 in VTP transparent mode (VTP disabled). These are extended-range VLANs and configuration options are limited. Extended-range VLANs are not saved in the VLAN database. See the “Configuring Extended-Range VLANs” section on page 11-11.
- Before you can create a VLAN, the switch must be in VTP server mode or VTP transparent mode. If the switch is a VTP server, you must define a VTP domain or VTP will not function.
- The switch does 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.
- The switch supports 128 spanning-tree instances. If a switch has more active VLANs than supported spanning-tree instances, spanning tree can be enabled on 128 VLANs and is disabled on the remaining VLANs. If you have already used all available spanning-tree instances on a switch, adding another VLAN anywhere in the VTP domain creates a VLAN on that switch that is not running spanning-tree. If you have the default allowed list on the trunk ports of that switch (which is to allow all VLANs), 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 would not be broken, particularly if there are several adjacent switches that all have run out of spanning-tree instances. You can prevent this possibility by setting allowed lists on the trunk ports of switches that have used up their allocation of spanning-tree instances.

If the number of VLANs on the switch exceeds the number of supported spanning tree instances, we recommend that you configure the IEEE 802.1s Multiple STP (MSTP) on your switch to map multiple VLANs to a single STP instance. For more information about MSTP, see Chapter 17, “Configuring MSTP.”

- To access VLAN configuration mode, enter the `vlan` global configuration command with a VLAN ID. Enter a new VLAN ID to create a VLAN, or enter an existing VLAN ID to modify the VLAN. You can use the default VLAN configuration (Table 11-2) or enter multiple commands to configure the VLAN. For more information about commands available in this mode, see the `vlan` global
configuration command description in the command reference for this release. When you have finished the configuration, you must exit VLAN configuration mode for the configuration to take effect. To display the VLAN configuration, enter the `show vlan` privileged EXEC command.

**Saving VLAN Configuration**

The configurations of VLAN IDs 1 to 1005 are always saved in the VLAN database (vlan.dat file). If VTP mode is transparent, they are also saved in the switch running configuration file and you can enter the `copy running-config startup-config` privileged EXEC command to save the configuration in the startup configuration file. You can use the `show running-config` privileged EXEC command to display the switch running configuration file. To display the VLAN configuration, enter the `show vlan` privileged EXEC command.

When you save VLAN and VTP information (including extended-range VLAN configuration information) in the startup configuration file and reboot the switch, the switch configuration is determined in these ways:

- If the VTP mode is transparent in the startup configuration, and the VLAN database and the VTP domain name from the VLAN database matches that in the startup configuration file, the VLAN database is ignored (cleared), and the VTP and VLAN configurations in the startup configuration file are used. The VLAN database revision number remains unchanged in the VLAN database.
- If the VTP mode or domain name in the startup configuration does not match the VLAN database, the domain name and VTP mode and configuration for the first 1005 VLANs use the VLAN database information.
- If VTP mode is server, the domain name and VLAN configuration for the first 1005 VLANs use the VLAN database information.

---

**Caution**

If the VLAN database configuration is used at startup and the startup configuration file contains extended-range VLAN configuration, this information is lost when the system boots up.

**Default Ethernet VLAN Configuration**

Table 11-2 shows the default configuration for Ethernet VLANs.

**Note**

The switch supports Ethernet interfaces exclusively. Because FDDI and Token Ring VLANs are not locally supported, you only configure FDDI and Token Ring media-specific characteristics for VTP global advertisements to other switches.
Table 11-2 Ethernet VLAN Defaults and Ranges

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN ID</td>
<td>1</td>
<td>1 to 4094.</td>
</tr>
<tr>
<td>Note</td>
<td>Extended-range VLANs (VLAN IDs 1006 to 4094) are not saved in the VLAN database.</td>
<td></td>
</tr>
<tr>
<td>VLAN name</td>
<td>VLANxxxx, where xxxx represents four numeric digits (including leading zeros) equal to the VLAN ID number</td>
<td>No range</td>
</tr>
<tr>
<td>802.10 SAID</td>
<td>100001 (100000 plus the VLAN ID)</td>
<td>1–4294967294</td>
</tr>
<tr>
<td>MTU size</td>
<td>1500</td>
<td>1500–18190</td>
</tr>
<tr>
<td>Translational bridge 1</td>
<td>0</td>
<td>0–1005</td>
</tr>
<tr>
<td>Translational bridge 2</td>
<td>0</td>
<td>0–1005</td>
</tr>
<tr>
<td>VLAN state</td>
<td>active</td>
<td>active, suspend</td>
</tr>
<tr>
<td>Remote SPAN</td>
<td>disabled</td>
<td>enabled, disabled</td>
</tr>
<tr>
<td>Private VLANs</td>
<td>none configured</td>
<td>2 to 1001, 1006 to 4094.</td>
</tr>
</tbody>
</table>

Creating or Modifying an Ethernet VLAN

Each Ethernet VLAN in the VLAN database has a unique, 4-digit ID that can be a number from 1 to 1001. VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs. To create a normal-range VLAN to be added to the VLAN database, assign a number and name to the VLAN.

**Note**

When the switch is in VTP transparent mode, you can assign VLAN IDs greater than 1006, but they are not added to the VLAN database. See the “Configuring Extended-Range VLANs” section on page 11-11.

For the list of default parameters that are assigned when you add a VLAN, see the “Configuring Normal-Range VLANs” section on page 11-4.

Beginning in privileged EXEC mode, follow these steps to create or modify an Ethernet VLAN:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td></td>
</tr>
<tr>
<td>vlan vlan-id</td>
<td>Enter a VLAN ID, and enter VLAN configuration mode. Enter a new VLAN ID to create a VLAN, or enter an existing VLAN ID to modify a VLAN.</td>
</tr>
<tr>
<td>Note</td>
<td>The available VLAN ID range for this command is 1 to 4094. For information about adding VLAN IDs greater than 1005 (extended-range VLANs), see the “Configuring Extended-Range VLANs” section on page 11-11.</td>
</tr>
</tbody>
</table>
Configuring Normal-Range VLANs

To return the VLAN name to the default settings, use the no name, no mtu, or no remote-span VLAN configuration commands.

This example shows how to create Ethernet VLAN 20, name it test20, and add it to the VLAN database:

```
Switch# configure terminal
Switch(config)# vlan 20
Switch(config-vlan)# name test20
Switch(config-vlan)# end
```

Deleting a VLAN

When you delete a VLAN from a switch that is in VTP server mode, the VLAN is removed from the VLAN database for 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 by using global configuration mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>no vlan vlan-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
</tr>
</tbody>
</table>
Assigning Static-Access Ports to a VLAN

You can assign a static-access port to a VLAN without having VTP globally propagate VLAN configuration information by disabling VTP (VTP transparent mode).

If you are assigning a port on a cluster member switch to a VLAN, first use the `rcommand privileged EXEC` command to log in to the cluster member switch.

**Note** If you assign an interface to a VLAN that does not exist, the new VLAN is created. (See the “Creating or Modifying an Ethernet VLAN” section on page 11-8.)

Beginning in privileged EXEC mode, follow these steps to assign a port to a VLAN in the VLAN database:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code> Enter global configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>interface interface-id</code> Enter the interface to be added to the VLAN.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>switchport mode access</code> Define the VLAN membership mode for the port (Layer 2 access port).</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>switchport access vlan vlan-id</code> Assign the port to a VLAN. Valid VLAN IDs are 1 to 4094.</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>end</code> Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 6</td>
<td><code>show running-config interface interface-id</code> Verify the VLAN membership mode of the interface.</td>
</tr>
<tr>
<td>Step 7</td>
<td><code>show interfaces interface-id switchport</code> Verify your entries in the Administrative Mode and the Access Mode VLAN fields of the display.</td>
</tr>
<tr>
<td>Step 8</td>
<td><code>copy running-config startup-config</code> (Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return an interface to its default configuration, use the `default interface interface-id` interface configuration command.

This example shows how to configure a port as an access port in VLAN 2:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 2
Switch(config-if)# end
```
Configuring Extended-Range VLANs

When the switch is in VTP transparent mode (VTP disabled), you can create extended-range VLANs (in the range 1006 to 4094). Extended-range VLANs enable service providers to extend their infrastructure to a greater number of customers. The extended-range VLAN IDs are allowed for any switchport commands that allow VLAN IDs.

Extended-range VLAN configurations are not stored in the VLAN database, but because VTP mode is transparent, they are stored in the switch running configuration file, and you can save the configuration in the startup configuration file by using the `copy running-config startup-config` privileged EXEC command.

**Note**

Although the switch supports 4094 VLAN IDs, see the “Supported VLANs” section on page 11-2 for the actual number of VLANs supported.

This section includes this information about extended-range VLANs:
- Default VLAN Configuration, page 11-11
- Extended-Range VLAN Configuration Guidelines, page 11-11
- Creating an Extended-Range VLAN, page 11-12
- Creating an Extended-Range VLAN with an Internal VLAN ID, page 11-13

Default VLAN Configuration

See Table 11-2 on page 11-8 for the default configuration for Ethernet VLANs. You can change only the MTU size and remote SPAN configuration state on extended-range VLANs; all other characteristics must remain at the default state.

Extended-Range VLAN Configuration Guidelines

Follow these guidelines when creating extended-range VLANs:
- To add an extended-range VLAN, you must use the `vlan vlan-id` global configuration command and access VLAN configuration mode. You cannot add extended-range VLANs in VLAN database configuration mode (accessed by entering the `vlan database` privileged EXEC command).
- VLAN IDs in the extended range are not saved in the VLAN database and are not recognized by VTP.
- You cannot include extended-range VLANs in the pruning eligible range.
- The switch must be in VTP transparent mode when you create extended-range VLANs. If VTP mode is server or client, an error message is generated, and the extended-range VLAN is rejected.
- You can set the VTP mode to transparent in global configuration mode or in VLAN database configuration mode. See the “Disabling VTP (VTP Transparent Mode)” section on page 12-10. You should save this configuration to the startup configuration so that the switch boots up in VTP transparent mode. Otherwise, you lose the extended-range VLAN configuration if the switch resets.
Configuring Extended-Range VLANs

- STP is enabled by default on extended-range VLANs, but you can disable it by using the no spanning-tree vlan vlan-id global configuration command. When the maximum number of spanning-tree instances (128) are on the switch, spanning tree is disabled on any newly created VLANs. If the number of VLANs on the switch exceeds the maximum number of spanning tree instances, we recommend that you configure the IEEE 802.1s Multiple STP (MSTP) on your switch to map multiple VLANs to a single STP instance. For more information about MSTP, see Chapter 17, “Configuring MSTP.”

- Each routed port on the switch creates an internal VLAN for its use. These internal VLANs use extended-range VLAN numbers, and the internal VLAN ID cannot be used for an extended-range VLAN. If you try to create an extended-range VLAN with a VLAN ID that is already allocated as an internal VLAN, an error message is generated, and the command is rejected.
  - Because internal VLAN IDs are in the lower part of the extended range, we recommend that you create extended-range VLANs beginning from the highest number (4094) and moving to the lowest (1006) to reduce the possibility of using an internal VLAN ID.
  - Before configuring extended-range VLANs, enter the show vlan internal usage privileged EXEC command to see which VLANs have been allocated as internal VLANs.
  - If necessary, you can shut down the routed port assigned to the internal VLAN, which frees up the internal VLAN, and then create the extended-range VLAN and re-enable the port, which then uses another VLAN as its internal VLAN. See the “Creating an Extended-Range VLAN with an Internal VLAN ID” section on page 11-13.

- Although the switch supports a total of 1005 (normal-range and extended-range) VLANs, the number of routed ports, SVIs, and other configured features affects the use of the switch hardware. If you try to create an extended-range VLAN and there are not enough hardware resources available, an error message is generated, and the extended-range VLAN is rejected.

Creating an Extended-Range VLAN

You create an extended-range VLAN in global configuration mode by entering the vlan global configuration command with a VLAN ID from 1006 to 4094. This command accesses the VLAN configuration mode. The extended-range VLAN has the default Ethernet VLAN characteristics (see Table 11-2) and the MTU size and RSPAN configuration are the only parameters you can change. See the description of the vlan global configuration command in the command reference for defaults of all parameters. If you enter an extended-range VLAN ID when the switch is not in VTP transparent mode, an error message is generated when you exit from VLAN configuration mode, and the extended-range VLAN is not created.

Extended-range VLANs are not saved in the VLAN database; they are saved in the switch running configuration file. You can save the extended-range VLAN configuration in the switch startup configuration file by using the copy running-config startup-config privileged EXEC command.

Note

Before you create an extended-range VLAN, you can verify that the VLAN ID is not used internally by entering the show vlan internal usage privileged EXEC command. If the VLAN ID is used internally and you want to free it up, go to the “Creating an Extended-Range VLAN with an Internal VLAN ID” section on page 11-13 before creating the extended-range VLAN.
Beginning in privileged EXEC mode, follow these steps to create an extended-range VLAN:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>vtp mode transparent</td>
<td>Configure the switch for VTP transparent mode, disabling VTP.</td>
</tr>
<tr>
<td>vlan vlan-id</td>
<td>Enter an extended-range VLAN ID and enter VLAN configuration mode. The range is 1006 to 4094.</td>
</tr>
<tr>
<td>mtu mtu-size</td>
<td>(Optional) Modify the VLAN by changing the MTU size. Note Although all VLAN commands appear in the CLI help in VLAN configuration mode, only the mtu mtu-size and remote-span commands are supported for extended-range VLANs.</td>
</tr>
<tr>
<td>remote-span</td>
<td>(Optional) Configure the VLAN as the RSPAN VLAN. See the “Configuring a VLAN as an RSPAN VLAN” section on page 28-16.</td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>show vlan id vlan-id</td>
<td>Verify that the VLAN has been created.</td>
</tr>
<tr>
<td>copy running-config startup config</td>
<td>Save your entries in the switch startup configuration file. To save extended-range VLAN configurations, you need to save the VTP transparent mode configuration and the extended-range VLAN configuration in the switch startup configuration file. Otherwise, if the switch resets, it will default to VTP server mode, and the extended-range VLAN IDs will not be saved.</td>
</tr>
</tbody>
</table>

To delete an extended-range VLAN, use the no vlan vlan-id global configuration command.

The procedure for assigning static-access ports to an extended-range VLAN is the same as for normal-range VLANs. See the “Assigning Static-Access Ports to a VLAN” section on page 11-10.

This example shows how to create a new extended-range VLAN with all default characteristics, enter VLAN configuration mode, and save the new VLAN in the switch startup configuration file:

```
Switch(config)# vtp mode transparent
Switch(config)# vlan 2000
Switch(config-vlan)# end
Switch# copy running-config startup config
```

**Creating an Extended-Range VLAN with an Internal VLAN ID**

If you enter an extended-range VLAN ID that is already assigned to an internal VLAN, an error message is generated, and the extended-range VLAN is rejected. To manually free an internal VLAN ID, you must temporarily shut down the routed port that is using the internal VLAN ID.
Beginning in privileged EXEC mode, follow these steps to release a VLAN ID that is assigned to an internal VLAN and to create an extended-range VLAN with that ID:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> show vlan internal usage</td>
<td>Display the VLAN IDs being used internally by the switch. If the VLAN ID that you want to use is an internal VLAN, the display shows the routed port that is using the VLAN ID. Enter that port number in Step 3.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong> interface interface-id</td>
<td>Enter the interface ID for the routed port that is using the VLAN ID.</td>
</tr>
<tr>
<td><strong>Step 4</strong> shutdown</td>
<td>Shut down the port to free the internal VLAN ID.</td>
</tr>
<tr>
<td><strong>Step 5</strong> exit</td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 6</strong> vtp mode transparent</td>
<td>Set the VTP mode to transparent for creating extended-range VLANs.</td>
</tr>
<tr>
<td><strong>Step 7</strong> vlan vlan-id</td>
<td>Enter the new extended-range VLAN ID, and enter VLAN configuration mode.</td>
</tr>
<tr>
<td><strong>Step 8</strong> exit</td>
<td>Exit from VLAN configuration mode, and return to global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 9</strong> interface interface-id</td>
<td>Enter the interface ID for the routed port that you shut down in Step 4.</td>
</tr>
<tr>
<td><strong>Step 10</strong> no shutdown</td>
<td>Re-enable the routed port. It will be assigned a new internal VLAN ID.</td>
</tr>
<tr>
<td><strong>Step 11</strong> end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 12</strong> copy running-config startup config</td>
<td>Save your entries in the switch startup configuration file. To save an extended-range VLAN configuration, you need to save the VTP transparent mode configuration and the extended-range VLAN configuration in the switch startup configuration file. Otherwise, if the switch resets, it will default to VTP server mode, and the extended-range VLAN IDs will not be saved.</td>
</tr>
</tbody>
</table>

### Displaying VLANs

Use the `show vlan` privileged EXEC command to display a list of all VLANs on the switch, including extended-range VLANs. The display includes VLAN status, ports, and configuration information. For a list of the VLAN IDs on the switch, use the `show vlan` privileged EXEC command.

Table 11-3 lists the privileged EXEC commands for monitoring VLANs.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show interfaces [vlan vlan-id]</td>
<td>Display characteristics for all interfaces or for the specified VLAN configured on the switch.</td>
</tr>
<tr>
<td>show vlan [id vlan-id]</td>
<td>Display parameters for all VLANs or the specified VLAN on the switch.</td>
</tr>
</tbody>
</table>

For more details about the show command options and explanations of output fields, see the command reference for this release.
Configuring VLAN Trunks

These sections describe how VLAN trunks function on the switch:

- Trunking Overview, page 11-15
- Encapsulation Types, page 11-16
- Default Layer 2 Ethernet Interface VLAN Configuration, page 11-18
- Configuring an Ethernet Interface as a Trunk Port, page 11-19
- Configuring Trunk Ports for Load Sharing, page 11-23

Trunking Overview

A trunk is a point-to-point link between one or more Ethernet switch interfaces and another networking device such as a router or a switch. Ethernet trunks carry the traffic of multiple VLANs over a single link, and you can extend the VLANs across an entire network.

Trunking encapsulation is available on 802.1Q Ethernet interfaces. 802.1Q is an industry-standard trunking encapsulation.

You can configure a trunk on a single Ethernet interface or on an EtherChannel bundle. For more information about EtherChannel, see Chapter 35, “Configuring EtherChannels and Link-State Tracking.”

Ethertone trunk interfaces support different trunking modes (see Table 11-4). You can set an interface as trunking or nontrunking or to negotiate trunking with the neighboring interface. To autonegotiate trunking, the interfaces must be in the same VTP domain.

Trunk negotiation is managed by the Dynamic Trunking Protocol (DTP), which is a Point-to-Point Protocol. However, some internetworking devices might forward DTP frames improperly, which could cause misconfigurations.

To avoid this, you should configure interfaces connected to devices that do not support DTP to not forward DTP frames, that is, to turn off DTP.

- If you do not intend to trunk across those links, use the switchport mode access interface configuration command to disable trunking.
- To enable trunking to a device that does not support DTP, use the switchport mode trunk and switchport nonegotiate interface configuration commands to cause the interface to become a trunk but to not generate DTP frames. Use the switchport trunk encapsulation dot1q interface to select the encapsulation type on the trunk port.

Note

Beginning with Cisco IOS Release 12.2(22)EY, ES ports support only 802.1 encapsulation. You cannot configure encapsulation on an ES port.

You can specify on standard DTP interfaces whether the trunk uses ISL or 802.1Q encapsulation or if the encapsulation type is autonegotiated. The DTP supports autonegotiation of 802.1Q trunks.

Note

DTP is not supported on private-VLAN ports or tunnel ports.
Tunnel ports do not support DTP. See Chapter 15, “Configuring IEEE 802.1Q and Layer 2 Protocol Tunneling,” for more information on tunnel ports.

### Table 11-4  Layer 2 Interface Modes

<table>
<thead>
<tr>
<th>Mode</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>switchport mode access</td>
<td>Puts the interface (access port) into permanent nontrunking mode and negotiates to convert the link into a nontrunk link. The interface becomes a nontrunk interface regardless of whether or not the neighboring interface is a trunk interface.</td>
</tr>
<tr>
<td>switchport mode dynamic auto</td>
<td>Makes the interface able to convert the link to a trunk link. The interface becomes a trunk interface if the neighboring interface is set to trunk or desirable mode. The default switchport mode for all Ethernet interfaces is dynamic auto.</td>
</tr>
<tr>
<td>switchport mode dynamic desirable</td>
<td>Makes the interface actively attempt to convert the link to a trunk link. The interface becomes a trunk interface if the neighboring interface is set to trunk, desirable, or auto mode.</td>
</tr>
<tr>
<td>switchport mode trunk</td>
<td>Puts the interface into permanent trunking mode and negotiates to convert the neighboring link into a trunk link. The interface becomes a trunk interface even if the neighboring interface is not a trunk interface.</td>
</tr>
<tr>
<td>switchport nonegotiate</td>
<td>Prevents the interface from generating DTP frames. You can use this command only when the interface switchport mode is access or trunk. You must manually configure the neighboring interface as a trunk interface to establish a trunk link.</td>
</tr>
<tr>
<td>switchport mode dot1q-tunnel</td>
<td>Configures the interface as a tunnel (nontrunking) port to be connected in an asymmetric link with an 802.1Q trunk port. 802.1Q tunneling is used to maintain customer VLAN integrity across a service provider network. See Chapter 15, “Configuring IEEE 802.1Q and Layer 2 Protocol Tunneling,” for more information on tunnel ports.</td>
</tr>
</tbody>
</table>

### Encapsulation Types

Table 11-5 lists the Ethernet trunk encapsulation types and keywords.

#### Table 11-5  Ethernet Trunk Encapsulation Types

<table>
<thead>
<tr>
<th>Encapsulation</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>switchport trunk encapsulation dot1q</td>
<td>Specifies 802.1Q encapsulation on the trunk link.</td>
</tr>
<tr>
<td>switchport trunk encapsulation isl</td>
<td>Specifies ISL encapsulation on the trunk link.</td>
</tr>
</tbody>
</table>

Beginning with Cisco IOS Release 12.2(22)EY, ISL trunks are not supported on ES ports. The encapsulation keyword is no longer visible for ES ports.
Note

The switch does not support Layer 3 trunks; you cannot configure subinterfaces or use the `encapsulation` keyword on Layer 3 interfaces. The switch does support Layer 2 trunks and Layer 3 VLAN interfaces, which provide equivalent capabilities.

Table 11-5  Ethernet Trunk Encapsulation Types (continued)

<table>
<thead>
<tr>
<th>Encapsulation</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>switchport trunk encapsulation negotiate</code></td>
<td>Specifies that the interface negotiate with the neighboring interface to become an ISL (preferred) or 802.1Q trunk, depending on the configuration and capabilities of the neighboring interface. This is the default for standard ports on the switch.</td>
</tr>
<tr>
<td><code>switchport trunk dot1q ethertype value</code></td>
<td>Sets the ethertype value for 802.1Q encapsulation. Used to select a nonstandard (nondefault) 2-byte ethertype to identify 802.1Q tagged frames. The default ethertype value is 0x8100. This option is supported only on enhanced-services (ES) ports.</td>
</tr>
</tbody>
</table>
IEEE 802.1Q Configuration Considerations

Note
Beginning with Cisco IOS Release 12.2(22)EY, ES ports only support IEEE 802.1Q trunking.

802.1Q trunks impose these limitations on the trunking strategy for a network:

- In a network of Cisco switches connected through 802.1Q trunks, the switches maintain one instance of spanning tree for each VLAN allowed on the trunks. Non-Cisco devices might support one spanning-tree instance for all VLANs.

  When you connect a Cisco switch to a non-Cisco device through an IEEE 802.1Q trunk, the Cisco switch combines the spanning-tree instance of the VLAN of the trunk with the spanning-tree instance of the non-Cisco 802.1Q switch. However, spanning-tree information for each VLAN is maintained by Cisco switches separated by a cloud of non-Cisco 802.1Q switches. The non-Cisco 802.1Q switch separates the Cisco switches is treated as a single trunk link between the switches.

- Make sure the native VLAN for an IEEE 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 spanning tree on the native VLAN of an IEEE 802.1Q trunk without disabling spanning tree on every VLAN in the network can potentially cause spanning-tree loops. We recommend that you leave spanning tree enabled on the native VLAN of an 802.1Q trunk or disable spanning tree on every VLAN in the network. Make sure your network is loop-free before disabling spanning tree.

- On an ES port, you can use the `switchport trunk dot1q ethertype value` interface configuration command to program a custom ethertype value for the interface. This feature allows the switch to interoperate with third-party vendor switches that do not use the standard 0x8100 ethertype to identify 802.1Q-tagged frames. For example, if you set 0x1234 as the custom IEEE 802.1Q ethertype on a trunk port, incoming frames containing that ethertype are assigned to the VLAN contained in the tag following the ethertype as they would be with a standard 802.1Q trunk. Frames arriving on a trunk port with either the standard ethertype (0x8100) or the custom ethertype value are treated as valid IEEE 802.1Q traffic; frames containing any other ethertype are assigned to the native VLAN of that trunk. Egress traffic that has an ethertype value of 0x8100 is mapped to the customer ethertype.

Default Layer 2 Ethernet Interface VLAN Configuration

Table 11-6 shows the default Layer 2 Ethernet interface VLAN configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface mode</td>
<td><code>switchport mode dynamic auto</code></td>
</tr>
<tr>
<td>Trunk encapsulation</td>
<td><code>switchport trunk encapsulation negotiate</code></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Beginning with Cisco IOS Release, this applies to only standard ports. ES ports support only 802.1Q encapsulation.</td>
</tr>
<tr>
<td>802.1Q encapsulation ethertype value</td>
<td>0x8100</td>
</tr>
<tr>
<td>Allowed VLAN range</td>
<td>VLANs 1 to 4094</td>
</tr>
</tbody>
</table>
Configuring an Ethernet Interface as a Trunk Port

Because trunk ports send and receive VTP advertisements, to use VTP 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.

This section includes these procedures for configuring an Ethernet interface as a trunk port on the switch:

- Interaction with Other Features, page 11-19
- Defining the Allowed VLANs on a Trunk, page 11-21
- Changing the Pruning-Eligible List, page 11-22
- Configuring the Native VLAN for Untagged Traffic, page 11-23

Note

By default, an interface is in Layer 2 mode. The default mode for Layer 2 interfaces is `switchport mode dynamic auto`. If the neighboring interface supports trunking and is configured to allow trunking, the link is a Layer 2 trunk or, if the interface is in Layer 3 mode, it becomes a Layer 2 trunk when you enter the `switchport` interface configuration command. By default, standard port trunks (or ES port trunks in release 12.1(14)AX) negotiate encapsulation. If the neighboring interface supports ISL and 802.1Q encapsulation and both interfaces are set to negotiate the encapsulation type, the trunk uses ISL encapsulation. Beginning with Cisco IOS Release 12.2(22)EY, ES ports support only 802.1Q encapsulation.

Interaction with Other Features

Trunking interacts with other features in these ways:

- A trunk port cannot be a secure port.
- A trunk port cannot be a tunnel port.
- Trunk ports can be grouped into EtherChannel port groups, but all trunks in the group must have the same configuration. 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 these parameters, the switch propagates the setting you entered to all ports in the group:
  
  - allowed-VLAN list
  - STP port priority for each VLAN
  - STP Port Fast setting
  - trunk status: if one port in a port group ceases to be a trunk, all ports cease to be trunks.

- We recommend that you configure no more than 24 trunk ports in PVST mode and no more than 40 trunk ports in MST mode.
If you try to enable 802.1x on a trunk port, an error message appears, and 802.1x is not enabled. If you try to change the mode of an 802.1x-enabled port to trunk, the port mode is not changed.

A port in dynamic mode can negotiate with its neighbor to become a trunk port. If you try to enable 802.1x on a dynamic port, an error message appears, and 802.1x is not enabled. If you try to change the mode of an 802.1x-enabled port to dynamic, the port mode is not changed.

### Configuring a Trunk Port

Beginning in privileged EXEC mode, follow these steps to configure a port as a trunk port:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td></td>
<td>Enter the interface configuration mode and the port to be configured for trunking.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>switchport trunk encapsulation {isl</td>
</tr>
<tr>
<td></td>
<td>Configure the port to support ISL or 802.1Q encapsulation or to negotiate (the default) with the neighboring interface for encapsulation type.</td>
</tr>
<tr>
<td></td>
<td>You must configure each end of the link with the same encapsulation type.</td>
</tr>
<tr>
<td></td>
<td>Note The encapsulation keyword is not supported on ES ports for Cisco IOS Release 12.2(22)EY and later. ES ports support only 802.1Q encapsulation.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>switchport mode {dynamic {auto</td>
</tr>
<tr>
<td></td>
<td>Configure the interface as a Layer 2 trunk (required only if the interface is a Layer 2 access port or tunnel port or to specify the trunking mode).</td>
</tr>
<tr>
<td></td>
<td>• dynamic auto—Set the interface to a trunk link if the neighboring interface is set to trunk or desirable mode. This is the default.</td>
</tr>
<tr>
<td></td>
<td>• dynamic desirable—Set the interface to a trunk link if the neighboring interface is set to trunk, desirable, or auto mode.</td>
</tr>
<tr>
<td></td>
<td>• trunk—Set the interface in permanent trunking mode and negotiate to convert the link to a trunk link even if the neighboring interface is not a trunk interface.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>switchport access vlan vlan-id (Optional)</td>
</tr>
<tr>
<td></td>
<td>Specify the default VLAN, which is used if the interface stops trunking.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>switchport trunk native vlan vlan-id</td>
</tr>
<tr>
<td></td>
<td>Specify the native VLAN for 802.1Q trunks.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>end</td>
</tr>
<tr>
<td></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>show interfaces interface-id switchport</td>
</tr>
<tr>
<td></td>
<td>Display the switchport configuration of the interface in the Administrative Mode and the Administrative Trunking Encapsulation fields of the display.</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>show interfaces interface-id trunk</td>
</tr>
<tr>
<td></td>
<td>Display the trunk configuration of the interface.</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>copy running-config startup-config (Optional)</td>
</tr>
<tr>
<td></td>
<td>Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return an interface to its default configuration, use the default interface interface-id interface configuration command. To reset all trunking characteristics of a trunking interface to the defaults, use the no switchport trunk interface configuration command. To disable trunking, use the switchport mode access interface configuration command to configure the port as a static-access port.
This example shows how to configure a standard port as an IEEE 802.1Q trunk. The example assumes that the neighbor interface is configured to support IEEE 802.1Q trunking.

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# switchport mode dynamic desirable
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# end
```

### Defining the Allowed VLANs on a Trunk

By default, a trunk port sends traffic to and receives traffic from all VLANs. All VLAN IDs, 1 to 4094, 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 `switchport trunk allowed vlan remove vlan-list` interface configuration command to remove specific VLANs from the allowed list.

---

**Note**

VLAN 1 is the default VLAN on all trunk ports in all Cisco switches, and it has previously been a requirement that VLAN 1 always be enabled on every trunk link. You can use the VLAN 1 minimization feature to disable VLAN 1 on any individual VLAN trunk link so that no user traffic (including spanning tree advertisements) is sent or received on VLAN 1.

---

To reduce the risk of spanning-tree loops or storms, you can disable VLAN 1 on any individual VLAN trunk port by removing VLAN 1 from the allowed list. When you remove VLAN 1 from a trunk port, the interface continues to send and receive management traffic, for example, Cisco Discovery Protocol (CDP), Port Aggregation Protocol (PAgP), Link Aggregation Control Protocol (LACP), Dynamic Trunking Protocol (DTP), and VLAN Trunking Protocol (VTP) in VLAN 1.

If a trunk port with VLAN 1 disabled is converted to a nontrunk port, it is added to the access VLAN. If the access VLAN is set to 1, the port will be added to VLAN 1, regardless of the `switchport trunk allowed` setting. The same is true for any VLAN that has been disabled on the port.

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 an ISL or 802.1Q trunk:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Enter interface configuration mode and the port to be configured.</td>
</tr>
<tr>
<td>Step 3 switchport mode trunk</td>
<td>Configure the interface as a VLAN trunk port.</td>
</tr>
</tbody>
</table>
### Configuring VLAN Trunks

#### Chapter 11      Configuring VLANs

**Configuring VLAN Trunks**

**To return to the default allowed VLAN list of all VLANs,** use the `no switchport trunk allowed vlan` interface configuration command.

**This example shows how to remove VLAN 2 from the allowed VLAN list on a port:**

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# switchport trunk allowed vlan remove 2
Switch(config-if)# end
```

**Changing the Pruning-Eligible List**

The pruning-eligible list applies only to trunk ports. Each trunk port has its own eligibility list. VTP pruning must be enabled for this procedure to take effect. The “Enabling VTP Pruning” section on page 12-12 describes how to enable VTP pruning.

Beginning in privileged EXEC mode, follow these steps to remove VLANs from the pruning-eligible list on a trunk port:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong> `switchport trunk allowed vlan {add</td>
<td>all</td>
</tr>
<tr>
<td><strong>Step 5</strong> <code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 6</strong> <code>show interfaces interface-id switchport</code></td>
<td>Verify your entries in the <em>Trunking VLANs Enabled</em> field of the display.</td>
</tr>
<tr>
<td><strong>Step 7</strong> <code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default allowed VLAN list of all VLANs, use the `no switchport trunk allowed vlan` interface configuration command.

This example shows how to remove VLAN 2 from the allowed VLAN list on a port:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# switchport trunk allowed vlan remove 2
Switch(config-if)# end
```

---

**Command Purpose**

**Step 1** `configure terminal` Enter global configuration mode.

**Step 2** `interface interface-id` Enter interface configuration mode, and select the trunk port for which VLANs should be pruned.

**Step 3** `switchport trunk pruning vlan {add | except | none | remove} vlan-list {vlan[,vlan[...]]}` Configure the list of VLANs allowed to be pruned from the trunk. (See the “VTP Pruning” section on page 12-4). For explanations about using the `add`, `except`, `none`, and `remove` keywords, see the command reference for this release. 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. Extended-range VLANs (VLAN IDs 1006 to 4094) cannot be pruned. VLANs that are pruning-ineligible receive flooded traffic. The default list of VLANs allowed to be pruned contains VLANs 2 to 1001.

**Step 4** `end` Return to privileged EXEC mode.
Chapter 11 Configuring VLANs

Configuring VLAN Trunks

Configuring VLAN Trunks

To return to the default pruning-eligible list of all VLANs, use the no switchport trunk pruning vlan interface configuration command.

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 in 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.

For information about 802.1Q configuration issues, see the “IEEE 802.1Q Configuration Considerations” section on page 11-18.

Beginning in privileged EXEC mode, follow these steps to configure the native VLAN on an 802.1Q trunk:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>switchport trunk native vlan vlan-id</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
</tr>
<tr>
<td>Step 5</td>
<td>show interfaces interface-id switchport</td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To return to the default native VLAN, VLAN 1, use the no switchport trunk native vlan interface configuration command.

If a packet has a VLAN ID that is the same as the outgoing port native VLAN ID, the packet is sent untagged; otherwise, the switch sends the packet with a tag.

Configuring Trunk Ports for Load Sharing

Load sharing divides the bandwidth supplied by parallel trunks connecting switches. To avoid loops, STP normally blocks all but one parallel link between switches. Using 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. For more information about STP, see Chapter 16, “Configuring STP.”

### 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 a blocking state. 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 sends or receives all traffic for the VLAN.

Figure 11-2 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 16 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 16 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 11-2 Load Sharing by Using STP Port Priorities**

![Diagram of two switches with trunks](image)

Beginning in privileged EXEC mode, follow these steps to configure the network shown in Figure 11-2.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: configure terminal</td>
<td>Enter global configuration mode on Switch A.</td>
</tr>
<tr>
<td>Step 2: vtp domain <em>domain-name</em></td>
<td>Configure a VTP administrative domain. The domain name can be from 1 to 32 characters.</td>
</tr>
<tr>
<td>Step 3: vtp mode server</td>
<td>Configure Switch A as the VTP server.</td>
</tr>
<tr>
<td>Step 4: end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
### Configuring VLAN Trunks

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td><code>show vtp status</code></td>
<td>Verify the VTP configuration on both Switch A and Switch B. In the display, check the VTP Operating Mode and the VTP Domain Name fields.</td>
</tr>
<tr>
<td>6</td>
<td><code>show vlan</code></td>
<td>Verify that the VLANs exist in the database on Switch A.</td>
</tr>
<tr>
<td>7</td>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>8</td>
<td><code>interface gigabitethernet1/0/1</code></td>
<td>Enter interface configuration mode, and define Gigabit Ethernet port 1 as the interface to be configured as a trunk.</td>
</tr>
<tr>
<td>9</td>
<td>`switchport trunk encapsulation {isl</td>
<td>dot1q</td>
</tr>
<tr>
<td>10</td>
<td><code>switchport mode trunk</code></td>
<td>Configure the port as a trunk port.</td>
</tr>
<tr>
<td>11</td>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>12</td>
<td><code>show interfaces gigabitethernet1/0/1 switchport</code></td>
<td>Verify the VLAN configuration.</td>
</tr>
<tr>
<td>13</td>
<td></td>
<td>Repeat Steps 7 through 11 on Switch A for a second interface in the switch.</td>
</tr>
<tr>
<td>14</td>
<td></td>
<td>Repeat Steps 7 through 11 on Switch B to configure the trunk ports that connect to the trunk ports configured on Switch A.</td>
</tr>
<tr>
<td>15</td>
<td><code>show vlan</code></td>
<td>When the trunk links come up, VTP passes the VTP and VLAN information to Switch B. Verify that Switch B has learned the VLAN configuration.</td>
</tr>
<tr>
<td>16</td>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode on Switch A.</td>
</tr>
<tr>
<td>17</td>
<td><code>interface gigabitethernet1/0/1</code></td>
<td>Enter interface configuration mode, and define the interface to set the STP port priority.</td>
</tr>
<tr>
<td>18</td>
<td><code>spanning-tree vlan 8-10 port-priority 16</code></td>
<td>Assign the port priority of 16 for VLANs 8 through 10.</td>
</tr>
<tr>
<td>19</td>
<td><code>exit</code></td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td>20</td>
<td><code>interface gigabitethernet1/0/2</code></td>
<td>Enter interface configuration mode, and define the interface to set the STP port priority.</td>
</tr>
<tr>
<td>21</td>
<td><code>spanning-tree vlan 3-6 port-priority 16</code></td>
<td>Assign the port priority of 16 for VLANs 3 through 6.</td>
</tr>
<tr>
<td>22</td>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>23</td>
<td><code>show running-config</code></td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>24</td>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
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, blocking different ports for different VLANs. The VLANs keep the traffic separate and maintain redundancy in the event of a lost link.

In Figure 11-3, Trunk ports 1 and 2 are configured as 100BASE-T ports. These VLAN path costs are assigned:

- VLANs 2 through 4 are assigned a path cost of 30 on Trunk port 1.
- VLANs 8 through 10 retain the default 100BASE-T 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 100BASE-T path cost on Trunk port 2 of 19.

### Figure 11-3 Load-Sharing Trunks with Traffic Distributed by Path Cost

Beginning in privileged EXEC mode, follow these steps to configure the network shown in Figure 11-3:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface gigabitethernet1/0/1</td>
</tr>
<tr>
<td>Step 3</td>
<td>switchport trunk encapsulation [isl</td>
</tr>
<tr>
<td>Step 4</td>
<td>switchport mode trunk</td>
</tr>
<tr>
<td>Step 5</td>
<td>exit</td>
</tr>
<tr>
<td>Step 6</td>
<td>end</td>
</tr>
<tr>
<td>Step 7</td>
<td>show running-config</td>
</tr>
</tbody>
</table>
### Configuring VMPS

The VLAN Query Protocol (VQP) is used to support dynamic-access ports, which are not permanently assigned to a VLAN, but given VLAN assignments based on the MAC source addresses seen on the port. Each time an unknown MAC address is seen, the switch sends a VQP query to a remote VMPS; the query includes the newly seen MAC address and the port on which it was seen. The VMPS responds with a VLAN assignment for the port. The switch cannot be a VMPS server but can act as a client to the VMPS and communicate with it through VQP.

This section includes this information about configuring VMPS:

- “Understanding VMPS” section on page 11-28
- “Default VMPS Client Configuration” section on page 11-29
- “VMPS Configuration Guidelines” section on page 11-29
- “Configuring the VMPS Client” section on page 11-30
- “Monitoring the VMPS” section on page 11-32
- “Troubleshooting Dynamic-Access Port VLAN Membership” section on page 11-33
- “VMPS Configuration Example” section on page 11-33

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 9  <code>show vlan</code></td>
<td>When the trunk links come up, Switch A receives the VTP information from the other switches. Verify that Switch A has learned the VLAN configuration.</td>
</tr>
<tr>
<td>Step 10 <code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 11 <code>interface gigabitethernet1/0/1</code></td>
<td>Enter interface configuration mode, and define Gigabit Ethernet port 1 as the interface on which to set the STP cost.</td>
</tr>
<tr>
<td>Step 12 <code>spanning-tree vlan 2-4 cost 30</code></td>
<td>Set the spanning-tree path cost to 30 for VLANs 2 through 4.</td>
</tr>
<tr>
<td>Step 13 <code>end</code></td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td>Step 14 <code>repeat</code></td>
<td>Repeat Steps 9 through 11 on the other configured trunk interface on Switch A, and set the spanning-tree path cost to 30 for VLANs 8, 9, and 10.</td>
</tr>
<tr>
<td>Step 15 <code>exit</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 16 <code>show running-config</code></td>
<td>Verify your entries. In the display, verify that the path costs are set correctly for both trunk interfaces.</td>
</tr>
<tr>
<td>Step 17 <code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
Understanding VMPS

Each time the client switch receives the MAC address of a new host, it sends a VQP query to the VMPS. When the VMPS receives this query, it searches its database for a MAC-address-to-VLAN mapping. The server response is based on this mapping and whether or not the server is in open or secure mode. In secure mode, the server shuts down the port when an illegal host is detected. In open mode, the server simply denies the host access to the port.

If the port is currently unassigned (that is, it does not yet have a VLAN assignment), the VMPS provides one of these responses:

- If the host is allowed on the port, the VMPS sends the client a vlan-assignment response containing the assigned VLAN name and allowing access to the host.
- If the host is not allowed on the port and the VMPS is in open mode, the VMPS sends an access-denied response.
- If the VLAN is not allowed on the port and the VMPS is in secure mode, the VMPS sends a port-shutdown response.

If the port already has a VLAN assignment, the VMPS provides one of these responses:

- If the VLAN in the database matches the current VLAN on the port, the VMPS sends an success response, allowing access to the host.
- If the VLAN in the database does not match the current VLAN on the port and active hosts exist on the port, the VMPS sends an access-denied or a port-shutdown response, depending on the secure mode of the VMPS.

If the switch receives an access-denied response from the VMPS, it continues to block traffic to and from the host MAC address. The switch continues to monitor the packets directed to the port and sends a query to the VMPS when it identifies a new host address. If the switch receives a port-shutdown response from the VMPS, it disables the port. The port must be manually re-enabled by using the CLI or SNMP.

Dynamic-Access Port VLAN Membership

A dynamic-access port can belong to only one VLAN with an ID from 1 to 4094. When the link comes up, the switch does not forward traffic to or from this port until the VMPS provides the VLAN assignment. The VMPS receives the source MAC address from the first packet of a new host connected to the dynamic-access port and attempts to match the MAC address to a VLAN in the VMPS database.

If there is a match, the VMPS sends the VLAN number for that port. If the client switch was not previously configured, it uses the domain name from the first VTP packet it receives on its trunk port from the VMPS. If the client switch was previously configured, it includes its domain name in the query packet to the VMPS to obtain its VLAN number. The VMPS verifies that the domain name in the packet matches its own domain name before accepting the request and responds to the client with the assigned VLAN number for the client. If there is no match, the VMPS either denies the request or shuts down the port (depending on the VMPS secure mode setting).

Multiple hosts (MAC addresses) can be active on a dynamic-access port if they are all in the same VLAN; however, the VMPS shuts down a dynamic-access port if more than 20 hosts are active on the port.

If the link goes down on a dynamic-access port, the port returns to an isolated state and does not belong to a VLAN. Any hosts that come online through the port are checked again through the VQP with the VMPS before the port is assigned to a VLAN.
Dynamic-access ports can be used for direct host connections, or they can connect to a network. A maximum of 20 MAC addresses are allowed per port on the switch. A dynamic-access port can belong to only one VLAN at a time, but the VLAN can change over time, depending on the MAC addresses seen.

**Default VMPS Client Configuration**

Table 11-7 shows the default VMPS and dynamic-access port configuration on client switches.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMPS domain server</td>
<td>None</td>
</tr>
<tr>
<td>VMPS reconfirm interval</td>
<td>60 minutes</td>
</tr>
<tr>
<td>VMPS server retry count</td>
<td>3</td>
</tr>
<tr>
<td>Dynamic-access ports</td>
<td>None configured</td>
</tr>
</tbody>
</table>

**VMPS Configuration Guidelines**

These guidelines and restrictions apply to dynamic-access port VLAN membership:

- You should configure the VMPS before you configure ports as dynamic-access ports.
- When you configure a port as a dynamic-access port, the spanning-tree Port Fast feature is automatically enabled for that port. The Port Fast mode accelerates the process of bringing the port into the forwarding state.
- 802.1x ports cannot be configured as dynamic-access ports. If you try to enable 802.1x on a dynamic-access (VQP) port, an error message appears, and 802.1x is not enabled. If you try to change an 802.1x-enabled port to dynamic VLAN assignment, an error message appears, and the VLAN configuration is not changed.
- Trunk ports cannot be dynamic-access ports, but you can enter the `switchport access vlan dynamic` interface configuration command for a trunk port. In this case, the switch retains the setting and applies it if the port is later configured as an access port.
  - You must turn off trunking on the port before the dynamic-access setting takes effect.
- Dynamic-access ports cannot be monitor ports.
- Secure ports cannot be dynamic-access ports. You must disable port security on a port before it becomes dynamic.
- Private VLAN ports cannot be dynamic-access ports.
- Dynamic-access ports cannot be members of an EtherChannel group.
- Port channels cannot be configured as dynamic-access ports.
- A dynamic-access port can participate in fallback bridging.
- The VTP management domain of the VMPS client and the VMPS server must be the same.
- The VLAN configured on the VMPS server should not be a voice VLAN.
Configuring the VMPS Client

You configure dynamic VLANs by using the VMPS (server). The switch can be a VMPS client; it cannot be a VMPS server.

Entering the IP Address of the VMPS

You must first enter the IP address of the server to configure the switch as a client.

Note
If the VMPS is being defined for a cluster of switches, enter the address on the command switch.

Beginning in privileged EXEC mode, follow these steps to enter the IP address of the VMPS:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 vmps server ipaddress primary</td>
<td>Enter the IP address of the switch acting as the primary VMPS server.</td>
</tr>
<tr>
<td>Step 3 vmps server ipaddress</td>
<td>(Optional) Enter the IP address of the switch acting as a secondary VMPS server. You can enter up to three secondary server addresses.</td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5 show vmps</td>
<td>Verify your entries in the VMPS Domain Server field of the display.</td>
</tr>
<tr>
<td>Step 6 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Note
You must have IP connectivity to the VMPS for dynamic-access ports to work. You can test for IP connectivity by pinging the IP address of the VMPS and verifying that you get a response.

Configuring Dynamic-Access Ports on VMPS Clients

If you are configuring a port on a cluster member switch as a dynamic-access port, first use the rcommand privileged EXEC command to log into the cluster member switch.

Caution
Dynamic-access port VLAN membership is for end stations or hubs connected to end stations. Connecting dynamic-access ports to other switches can cause a loss of connectivity.
Beginning in privileged EXEC mode, follow these steps to configure a dynamic-access port on a VMPS client switch:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>switchport mode access</td>
</tr>
<tr>
<td>Step 4</td>
<td>switchport access vlan dynamic</td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
</tr>
<tr>
<td>Step 6</td>
<td>show interfaces interface-id switchport</td>
</tr>
<tr>
<td>Step 7</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To return an interface to its default configuration, use the `default interface interface-id` interface configuration command. To return an interface to its default switchport mode (dynamic auto), use the `no switchport mode` interface configuration command. To reset the access mode to the default VLAN for the switch, use the `no switchport access vlan` interface configuration command.

### Reconfirming VLAN Memberships

Beginning in privileged EXEC mode, follow these steps to confirm the dynamic-access port VLAN membership assignments that the switch has received from the VMPS:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>vmps reconfirm</td>
</tr>
<tr>
<td>Step 2</td>
<td>show vmps</td>
</tr>
</tbody>
</table>

### Changing the Reconfirmation Interval

VMPS clients periodically reconfirm the VLAN membership information received from the VMPS. You can set the number of minutes after which reconfirmation occurs.

If you are configuring a member switch in a cluster, this parameter must be equal to or greater than the reconfirmation setting on the command switch. You must also first use the `rcommand` privileged EXEC command to log into the member switch.

Beginning in privileged EXEC mode, follow these steps to change the reconfirmation interval:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>vmps reconfirm minutes</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
</tr>
</tbody>
</table>
Configuring VMPS

To return the switch to its default setting, use the `no vmps reconfirm` global configuration command.

Changing the Retry Count

Beginning in privileged EXEC mode, follow these steps to change the number of times that the switch attempts to contact the VMPS before querying the next server:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>vmps retry count</code></td>
</tr>
<tr>
<td></td>
<td>Change the retry count. The retry range is from 1 to 10; the default is 3.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>end</code></td>
</tr>
<tr>
<td></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>show vmps</code></td>
</tr>
<tr>
<td></td>
<td>Verify your entry in the <code>Server Retry Count</code> field of the display.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>copy running-config startup-config</code></td>
</tr>
<tr>
<td></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return the switch to its default setting, use the `no vmps retry` global configuration command.

Monitoring the VMPS

You can display information about the VMPS by using the `show vmps` privileged EXEC command. The switch displays this information about the VMPS:

- **VMPS VQP Version**—the version of VQP used to communicate with the VMPS. The switch queries the VMPS that is using VQP Version 1.
- **Reconfirm Interval**—the number of minutes the switch waits before reconfirming the VLAN-to-MAC-address assignments.
- **Server Retry Count**—the number of times VQP resends a query to the VMPS. If no response is received after this many tries, the switch starts to query the secondary VMPS.
- **VMPS domain server**—the IP address of the configured VLAN membership policy servers. The switch sends queries to the one marked `current`. The one marked `primary` is the primary server.
- **VMPS Action**—the result of the most recent reconfirmation attempt. A reconfirmation attempt can occur automatically when the reconfirmation interval expired, or you can force it by entering the `vmps reconfirm` privileged EXEC command or its SNMP equivalent.
This is an example of output for the `show vmps` privileged EXEC command:

```
Switch# show vmps

VQP Client Status:
-------------------
VMPS VQP Version:   1
Reconfirm Interval: 60 min
Server Retry Count: 3
VMPS domain server: 172.20.128.86 (primary, current)
                    172.20.128.87

Reconfirmation status
---------------------
VMPS Action:         other
```

**Troubleshooting Dynamic-Access Port VLAN Membership**

The VMPS shuts down a dynamic-access port under these conditions:

- The VMPS is in secure mode, and it does not allow the host to connect to the port. The VMPS shuts down the port to prevent the host from connecting to the network.
- More than 20 active hosts reside on a dynamic-access port.

To re-enable a disabled dynamic-access port, enter the `shutdown` interface configuration command followed by the `no shutdown` interface configuration command.

**VMPS Configuration Example**

Figure 11-4 shows a network with a VMPS server switch and VMPS client switches with dynamic-access ports. In this example, these assumptions apply:

- The VMPS server and the VMPS client are separate switches.
- The Catalyst 6500 series Switch A is the primary VMPS server.
- The Catalyst 6500 series Switch C and Switch J are secondary VMPS servers.
- End stations are connected to the clients, Switch B and Switch I.
- The database configuration file is stored on the TFTP server with the IP address 172.20.22.7.
Figure 11-4  Dynamic Port VLAN Membership Configuration

Catalyst 6500 series switch A
Primary VMPS
Server 1
172.20.26.150

End
station 1
Dynamic-access port
Client switch B
172.20.26.151

Catalyst 6500 series
Secondary VMPS
Server 2
172.20.26.152

Switch D
172.20.26.153

Switch E
172.20.26.154

Switch F
172.20.26.155

Switch G
172.20.26.156

Switch H
172.20.26.157

End
station 2
Dynamic-access port
Client switch I
172.20.26.158

Catalyst 6500 series
Secondary VMPS
Server 3
172.20.26.159

Switch J

TFTP server
172.20.22.7

Router
Configuring VTP

This chapter describes how to use the VLAN Trunking Protocol (VTP) and the VLAN database for managing VLANs with the Catalyst 3750 Metro switch.

Note

For complete syntax and usage information for the commands used in this chapter, see the command reference for this release.

The chapter includes these sections:

- Understanding VTP, page 12-1
- Configuring VTP, page 12-6
- Monitoring VTP, page 12-13

Understanding VTP

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 one or more switches 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.

VTP is designed to work in an environment where updates are made on a single switch and are sent through VTP to other switches in the domain. It does not work well in a situation where multiple updates to the VLAN database occur simultaneously on switches in the same domain, which would result in an inconsistency in the VLAN database.

The switch supports 1005 VLANs, but the number of routed ports, SVIs, and other configured features affects the usage of the switch hardware. If the switch is notified by VTP of a new VLAN and the switch is already using the maximum available hardware resources, it sends a message that there are not enough hardware resources available and shuts down the VLAN. The output of the `show vlan` user EXEC command shows the VLAN in a suspended state.

VTP only learns about normal-range VLANs (VLAN IDs 1 to 1005). Extended-range VLANs (VLAN IDs greater than 1005) are not supported by VTP or stored in the VTP VLAN database.
This section contains information about these VTP parameters and characteristics.

- The VTP Domain, page 12-2
- VTP Modes, page 12-3
- VTP Advertisements, page 12-3
- VTP Version 2, page 12-4
- VTP Pruning, page 12-4

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 sharing the same VTP domain name. A switch can be in only one VTP domain. You make global VLAN configuration changes for the domain.

By default, the switch is in VTP 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. Until the management domain name is specified or learned, you cannot create or modify VLANs on a VTP server, and VLAN information is not propagated over the network.

If the switch receives a VTP advertisement over a trunk link, it inherits the management domain name and the VTP configuration revision number. The switch then ignores advertisements with a different domain name or an earlier configuration revision number.

Caution

Before adding a VTP client switch to a VTP domain, always verify that its VTP configuration revision number is lower than the configuration revision number of the other switches in the VTP domain.

Switches in a VTP domain always use the VLAN configuration of the switch with the highest VTP configuration revision number. If you add a switch that has a revision number higher than the revision number in the VTP domain, it can erase all VLAN information from the VTP server and VTP domain. See the “Adding a VTP Client Switch to a VTP Domain” section on page 12-12 for the procedure for verifying and resetting the VTP 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 IEEE trunk connections, including Inter-Switch Link (ISL) and IEEE 802.1Q. VTP dynamically maps VLANs with unique names and internal index associates across multiple LAN types. Mapping eliminates excessive device administration required from network administrators.

If you configure a switch for VTP transparent mode, you can create and modify VLANs, but the changes are not sent to other switches in the domain, and they affect only the individual switch. However, configuration changes made when the switch is in this mode are saved in the switch running configuration and can be saved to the switch startup configuration file.

For domain name and password configuration guidelines, see the “VTP Configuration Guidelines” section on page 12-6.
VTP Modes

You can configure a supported switch to be in one of the VTP modes listed in Table 12-1.

<table>
<thead>
<tr>
<th>VTP Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VTP server</td>
<td>In VTP server mode, you can create, modify, and delete VLANs, and specify other configuration parameters (such as the 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. In VTP server mode, VLAN configurations are saved in NVRAM. VTP server is the default mode.</td>
</tr>
<tr>
<td>VTP client</td>
<td>A VTP client behaves like a VTP server and transmits and receives VTP updates on its trunks, but you cannot create, change, or delete VLANs on a VTP client. VLANs are configured on another switch in the domain that is in server mode. In VTP client mode, VLAN configurations are not saved in NVRAM.</td>
</tr>
<tr>
<td>VTP transparent</td>
<td>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, in VTP Version 2, transparent switches do forward VTP advertisements that they receive from other switches from their trunk interfaces. You can create, modify, and delete VLANs on a switch in VTP transparent mode. The switch must be in VTP transparent mode when you create extended-range VLANs. See the “Configuring Extended-Range VLANs” section on page 11-11. The switch must be in VTP transparent mode when you create private VLANs. See Chapter 13, “Configuring Private VLANs.” When private VLANs are configured, do not change the VTP mode from transparent to client or server mode. When the switch is in VTP transparent mode, the VTP and VLAN configurations are saved in NVRAM, but they are not advertised to other switches. In this mode, VTP mode and domain name are saved in the switch running configuration and you can save this information in the switch startup configuration file by entering the <code>copy running-config startup-config</code> privileged EXEC command.</td>
</tr>
</tbody>
</table>

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 another switch. Otherwise, the switch cannot receive any VTP advertisements. For more information on trunk ports, see the “Configuring VLAN Trunks” section on page 11-15.

VTP advertisements distribute this global domain information:

- VTP domain name
- VTP configuration revision number
- Update identity and update timestamp
• MD5 digest VLAN configuration, including maximum transmission unit (MTU) size for each VLAN.
• Frame format

VTP advertisements distribute this VLAN information for each configured VLAN:
• VLAN IDs (ISL and 802.1Q)
• VLAN name
• VLAN type
• VLAN state
• Additional VLAN configuration information specific to the VLAN type

**VTP Version 2**

If you use VTP in your network, you must decide whether to use Version 1 or Version 2. By default, VTP operates in Version 1.

VTP Version 2 supports these features not supported in Version 1:
• Token Ring support—VTP Version 2 supports Token Ring Bridge Relay Function (TrBRF) and Token Ring Concentrator Relay Function (TrCRF) VLANs. For more information about Token Ring VLANs, see the “Configuring Normal-Range VLANs” section on page 11-4.
• 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 NVRAM 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. Although VTP version 2 supports only one domain, a VTP version 2 transparent switch forwards a message only when the domain name matches.
• 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 or SNMP. Consistency checks are not performed when new information is obtained from a VTP message or when information is read from NVRAM. If the MD5 digest on a received VTP message is correct, its information is accepted.

**VTP Pruning**

VTP pruning increases network available bandwidth by restricting flooded traffic to those trunk links that the traffic must use to reach the destination devices. Without VTP pruning, a switch floods broadcast, multicast, and unknown unicast traffic across all trunk links within a VTP domain even though receiving switches might discard them. VTP pruning is disabled by default.

VTP pruning blocks unneeded flooded traffic to VLANs on trunk ports that are included in the pruning-eligible list. Only VLANs included in the pruning-eligible list can be pruned. By default, VLANs 2 through 1001 are pruning eligible switch trunk ports. If the VLANs are configured as pruning-ineligible, the flooding continues. VTP pruning is supported with VTP Version 1 and Version 2.

*Figure 12-1* shows a switched network without VTP pruning enabled. Port 1 on Switch A and Port 2 on Switch D are assigned to the Red VLAN. If a broadcast is sent from the host connected to Switch A, Switch A floods the broadcast and every switch in the network receives it, even though Switches C, E, and F have no ports in the Red VLAN.
Understanding VTP

Figure 12-1  Flooding Traffic without VTP Pruning

Figure 12-2  shows a switched network with VTP pruning enabled. The broadcast traffic from Switch A is not forwarded to Switches C, E, and F because traffic for the Red VLAN has been pruned on the links shown (Port 5 on Switch B and Port 4 on Switch D).

Figure 12-2  Optimized Flooded Traffic with VTP Pruning

Enabling VTP pruning on a VTP server enables pruning for the entire management domain. Making VLANs pruning-eligible or pruning-ineligible affects pruning eligibility for those VLANs on that trunk only (not on all switches in the VTP domain).

See the “Enabling VTP Pruning” section on page 12-12. VTP pruning takes effect several seconds after you enable it. VTP pruning does not prune traffic from VLANs that are pruning-ineligible. VLAN 1 and VLANs 1002 to 1005 are always pruning-ineligible; traffic from these VLANs cannot be pruned. Extended-range VLANs (VLAN IDs higher than 1005) are also pruning-ineligible.
VTP pruning is not designed to function in VTP transparent mode. If one or more switches in the network are in VTP transparent mode, you should do one of these:

- Turn off VTP pruning in the entire network.
- Turn off VTP pruning by making all VLANs on the trunk of the switch upstream to the VTP transparent switch pruning ineligible.

To configure VTP pruning on an interface, use the `switchport trunk pruning vlan` interface configuration command (see the “Changing the Pruning-Eligible List” section on page 11-22). VTP pruning operates when an interface is trunking. You can set VLAN pruning-eligibility, whether or not VTP pruning is enabled for the VTP domain, whether or not any given VLAN exists, and whether or not the interface is currently trunking.

## Configuring VTP

This section includes guidelines and procedures for configuring VTP. These sections are included:

- Default VTP Configuration, page 12-6
- VTP Configuration Guidelines, page 12-6
- Configuring a VTP Server, page 12-8
- Configuring a VTP Client, page 12-9
- Disabling VTP (VTP Transparent Mode), page 12-10
- Enabling VTP Version 2, page 12-11
- Enabling VTP Pruning, page 12-12
- Adding a VTP Client Switch to a VTP Domain, page 12-12

### Default VTP Configuration

Table 12-2 shows the default VTP configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>VTP domain name</td>
<td>Null.</td>
</tr>
<tr>
<td>VTP mode</td>
<td>Server.</td>
</tr>
<tr>
<td>VTP version</td>
<td>Version 1 (Version 2 is disabled).</td>
</tr>
<tr>
<td>VTP password</td>
<td>None.</td>
</tr>
<tr>
<td>VTP pruning</td>
<td>Disabled.</td>
</tr>
</tbody>
</table>

### VTP Configuration Guidelines

You use the `vtp` global configuration command to set the VTP password, the version, the VTP file name, the interface providing updated VTP information, the domain name, and the mode, and to disable or enable pruning. For more information about available keywords, see the command descriptions in the command reference for this release. The VTP information is saved in the VTP VLAN database. When
VTP mode is transparent, the VTP domain name and mode are also saved in the switch running configuration file, and you can save it in the switch startup configuration file by entering the `copy running-config startup-config` privileged EXEC command. You must use this command if you want to save VTP mode as transparent, even if the switch resets.

When you save VTP information in the switch startup configuration file and reboot the switch, the switch configuration is determined as follows:

- If the VTP mode is transparent in the startup configuration and the VLAN database and the VTP domain name from the VLAN database matches that in the startup configuration file, the VLAN database is ignored (cleared), and the VTP and VLAN configurations in the startup configuration file are used. The VLAN database revision number remains unchanged in the VLAN database.
- If the VTP mode or domain name in the startup configuration do not match the VLAN database, the domain name and VTP mode and configuration for the first 1005 VLANs use the VLAN database information.

These sections describe guidelines you should follow when implementing VTP in your network.

**Domain Names**

When configuring VTP for the first time, you must always assign a domain name. You must configure all switches in the VTP domain 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.

**Note**

If NVRAM and DRAM storage is sufficient, all switches in a VTP domain should be in VTP server mode.

**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. Make sure that 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. If you do configure a domain password, all domain switches must share the same password and you must configure the password on each switch in the management domain. Switches without a password or with the wrong password reject VTP advertisements.

If you configure a VTP password for a domain, a 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 with VTP capability, the new switch learns the domain name only after the applicable password has been configured on it.

**Caution**

When you configure a VTP domain password, the management domain does not function properly if you do not assign a management domain password to each switch in the domain.
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 does not exchange VTP information with switches with Version 2 enabled.
- If there are TrBRF and TrCRF Token Ring networks in your environment, 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.

Configuration Requirements

When you configure VTP, you must configure a trunk port so that the switch can send and receive VTP advertisements to and from other switches in the domain.

For more information, see the “Configuring VLAN Trunks” section on page 11-15.

If you are configuring VTP on a cluster member switch to a VLAN, use the `rcommand` privileged EXEC command to log into the member switch. For more information about the command, see the command reference for this release.

If you are configuring extended-range VLANs on the switch, the switch must be in VTP transparent mode.

VTP does not support private VLANs. If you configure private VLANs, the switch must be in VTP transparent mode. When private VLANs are configured on the switch, do not change the VTP mode from transparent to client or server mode.

Configuring a VTP Server

When a switch is in VTP server mode, you can change the VLAN configuration and have it propagated throughout the network.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>vtp domain <code>domain-name</code></td>
<td>Configure the VTP administrative-domain name. The name can be from 1 to 32 characters. All switches operating in VTP server or client mode under the same administrative responsibility must be configured with the same domain name.</td>
</tr>
<tr>
<td>Step 3</td>
<td>vtp mode server</td>
<td>Configure the switch for VTP server mode (the default).</td>
</tr>
</tbody>
</table>

Note: If extended-range VLANs are configured on the switch, you cannot change VTP mode to server. You receive an error message, and the configuration is not allowed.

Beginning in privileged EXEC mode, follow these steps to configure the switch as a VTP server:
When you configure a domain name, it cannot be removed; you can only reassign a switch to a different domain.

To return the switch to a no-password state, use the `no vtp password` global configuration command.

This example shows how to use global configuration mode to configure the switch as a VTP server with the domain name `eng_group` and the password `mypassword`:

```
Switch# config terminal
Switch(config)# vtp domain eng_group
Switch(config)# vtp mode server
Switch(config)# vtp password mypassword
Switch(config)# end
```

### Configuring a VTP Client

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.

Follow these guidelines:

- If extended-range VLANs are configured on the switch, you cannot change VTP mode to client. You receive an error message, and the configuration is not allowed.

- If you configure the switch for VTP client mode, the switch does not create the VLAN database file (`vlan.dat`). If the switch is then powered off, it resets the VTP configuration to the default. To keep the VTP configuration with VTP client mode after the switch restarts, you must first configure the VTP domain name before the VTP mode.

⚠️ **Caution**

If all switches are operating in VTP client mode, do not configure a VTP domain name. If you do, it is impossible to make changes to the VLAN configuration of that domain. Therefore, make sure you configure at least one switch as a VTP server.
Beginning in privileged EXEC mode, follow these steps to configure the switch as a VTP client:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>vtp domain <em>domain-name</em></td>
</tr>
<tr>
<td>Step 3</td>
<td>vtp mode client</td>
</tr>
<tr>
<td>Step 4</td>
<td>vtp password <em>password</em></td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
</tr>
<tr>
<td>Step 6</td>
<td>show vtp status</td>
</tr>
</tbody>
</table>

Use the **no vtp mode** global configuration command to return the switch to VTP server mode. To return the switch to a no-password state, use the **no vtp password** privileged EXEC command. When you configure a domain name, it cannot be removed; you can only reassign a switch to a different domain.

**Disabling VTP (VTP Transparent Mode)**

When you configure the switch for VTP transparent mode, you disable VTP on the switch. The switch does not send VTP updates and does not act on VTP updates received from other switches. However, a VTP transparent switch running VTP Version 2 does forward received VTP advertisements on all of its trunk links.

**Note**

Before you create extended-range VLANs (VLAN IDs 1006 to 4094), you must set VTP mode to transparent by using the **vtp mode transparent** global configuration command. Save this configuration to the startup configuration so that the switch boots up in VTP transparent mode. Otherwise, you lose the extended-range VLAN configuration if the switch resets and boots up in VTP server mode (the default).

Beginning in privileged EXEC mode, follow these steps to configure VTP transparent mode and save the VTP configuration in the switch startup configuration file:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>vtp mode transparent</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
</tr>
</tbody>
</table>
Chapter 12 Configuring VTP

Configuring VTP

To return the switch to VTP server mode, use the no vtp mode global configuration command.

Note

If extended-range VLANs are configured on the switch, you cannot change the VTP mode to server. You receive an error message, and the configuration is not allowed.

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. You can only configure the version on switches in VTP server or transparent mode.

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 TrCRF and TrBRF Token ring environments, you must enable VTP Version 2 for Token Ring VLAN switching to function properly. For Token Ring and Token Ring-Net media, VTP Version 2 must be disabled.

For more information on VTP version configuration guidelines, see the “VTP Version” section on page 12-8.

Beginning in privileged EXEC mode, follow these steps to enable VTP Version 2:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 vtp version 2</td>
<td>Enable VTP Version 2 on the switch.</td>
</tr>
<tr>
<td>Step 3 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4 show vtp status</td>
<td>Verify that VTP Version 2 is enabled in the VTP V2 Mode field of the display.</td>
</tr>
</tbody>
</table>

To disable VTP Version 2, use the no vtp version global configuration command.
Enabling VTP Pruning

Pruning increases available bandwidth by restricting flooded traffic to those trunk links that the traffic must use to access the destination devices. You can only enable VTP pruning on a switch in VTP server mode.

Beginning in privileged EXEC mode, follow these steps to enable VTP pruning in the VTP domain:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>vtp pruning</td>
</tr>
<tr>
<td></td>
<td>Enable pruning in the VTP administrative domain.</td>
</tr>
<tr>
<td></td>
<td>By default, pruning is disabled. You need to enable pruning on only one switch in VTP server mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
</tr>
<tr>
<td></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show vtp status</td>
</tr>
<tr>
<td></td>
<td>Verify your entries in the VTP Pruning Mode field of the display.</td>
</tr>
</tbody>
</table>

To disable VTP pruning, use the no vtp pruning global configuration command.

Pruning is supported with VTP Version 1 and Version 2. If you enable pruning on the VTP server, it is enabled for the entire VTP domain.

Only VLANs included in the pruning-eligible list can be pruned. By default, VLANs 2 through 1001 are pruning eligible on trunk ports. Reserved VLANs and extended-range VLANs cannot be pruned. To change the pruning-eligible VLANs, see the “Changing the Pruning-Eligible List” section on page 11-22.

Adding a VTP Client Switch to a VTP Domain

Before adding a VTP client to a VTP domain, always verify that its VTP configuration revision number is lower than the configuration revision number of the other switches in the VTP domain. Switches in a VTP domain always use the VLAN configuration of the switch with the highest VTP configuration revision number. If you add a switch that has a revision number higher than the revision number in the VTP domain, it can erase all VLAN information from the VTP server and VTP domain.

Beginning in privileged EXEC mode, follow these steps to verify and reset the VTP configuration revision number on a switch before adding it to a VTP domain:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>show vtp status</td>
</tr>
<tr>
<td></td>
<td>Check the VTP configuration revision number.</td>
</tr>
<tr>
<td></td>
<td>If the number is 0, add the switch to the VTP domain.</td>
</tr>
<tr>
<td></td>
<td>If the number is greater than 0, follow these steps:</td>
</tr>
<tr>
<td></td>
<td>a. Write down the domain name.</td>
</tr>
<tr>
<td></td>
<td>b. Write down the configuration revision number.</td>
</tr>
<tr>
<td></td>
<td>c. Continue with the next steps to reset the switch configuration revision number.</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>vtp domain domain-name</td>
</tr>
<tr>
<td></td>
<td>Change the domain name from the original one displayed in Step 1 to a new name.</td>
</tr>
</tbody>
</table>
After resetting the configuration revision number, add the switch to the VTP domain.

**Note**
You can use the `vtp mode transparent` global configuration command or the `vtp transparent` VLAN database configuration command to disable VTP on the switch, and then change its VLAN information without affecting the other switches in the VTP domain.

## Monitoring VTP

You monitor VTP by displaying VTP 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.

Table 12-3 shows the privileged EXEC commands for monitoring VTP activity.

### Table 12-3  VTP Monitoring Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show vtp status</code></td>
<td>Display the VTP switch configuration information.</td>
</tr>
<tr>
<td><code>show vtp counters</code></td>
<td>Display counters about VTP messages that have been sent and received.</td>
</tr>
</tbody>
</table>
CHAPTER 13

Configuring Private VLANs

This chapter describes how to configure private VLANs on the Catalyst 3750 Metro switch.

Note

For complete syntax and usage information for the commands used in this chapter, see the command reference for this release.

The chapter includes these sections:

- Understanding Private VLANs, page 13-1
- Configuring Private VLANs, page 13-6
- Monitoring Private VLANs, page 13-14

Note

When you configure private VLANs, the switch must be in VTP transparent mode. See Chapter 12, “Configuring VTP.”

Understanding Private VLANs

The private-VLAN feature addresses two problems that service providers face when using VLANs:

- Scalability: The switch supports up to 1005 active VLANs. If a service provider assigns one VLAN per customer, this limits the numbers of customers that the service provider can support.
- To enable IP routing, each VLAN is assigned a subnet address space or a block of addresses, which can waste the unused IP addresses and cause IP address management problems.

Using private VLANs addresses the scalability problem and provides IP address management benefits for service providers and Layer 2 security for customers. Private VLANs partition a regular VLAN domain into subdomains. A subdomain is represented by a pair of VLANs: a primary VLAN and a secondary VLAN. A private VLAN can have multiple VLAN pairs, one pair for each subdomain. All VLAN pairs in a private VLAN share the same primary VLAN. The secondary VLAN ID differentiates one subdomain from another. See Figure 13-1.
Figure 13-1  Private-VLAN Domain

There are two types of secondary VLANs:
- **Isolated VLANs**—Ports within an isolated VLAN cannot communicate with each other at the Layer 2 level.
- **Community VLANs**—Ports within a community VLAN can communicate with each other but cannot communicate with ports in other communities at the Layer 2 level.

Private VLANs provide Layer 2 isolation between ports within the same private VLAN. Private-VLAN ports are access ports that are one of these types:
- **Promiscuous**—A promiscuous port belongs to the primary VLAN and can communicate with all interfaces, including the community and isolated host ports that belong to the secondary VLANs associated with the primary VLAN.
- **Isolated**—An isolated port is a host port that belongs to an isolated secondary VLAN. It has complete Layer 2 separation from other ports within the same private VLAN, except for the promiscuous ports. Private VLANs block all traffic to isolated ports except traffic from promiscuous ports. Traffic received from an isolated port is forwarded only to promiscuous ports.
- **Community**—A community port is a host port that belongs to a community secondary VLAN. Community ports communicate with other ports in the same community VLAN and with promiscuous ports. These interfaces are isolated at Layer 2 from all other interfaces in other communities and from isolated ports within their private VLAN.

*Note*  Trunk ports carry traffic from regular VLANs and also from primary, isolated, and community VLANs.
Primary and secondary VLANs have these characteristics:

- **Primary VLAN**—A private VLAN has only one primary VLAN. Every port in a private VLAN is a member of the primary VLAN. The primary VLAN carries unidirectional traffic downstream from the promiscuous ports to the (isolated and community) host ports and to other promiscuous ports.

- **Isolated VLAN**—A private VLAN has only one isolated VLAN. An isolated VLAN is a secondary VLAN that carries unidirectional traffic upstream from the hosts toward the promiscuous ports and the gateway.

- **Community VLAN**—A community VLAN is a secondary VLAN that carries upstream traffic from the community ports to the promiscuous port gateways and to other host ports in the same community. You can configure multiple community VLANs in a private VLAN.

A promiscuous port can serve only one primary VLAN, one isolated VLAN, and multiple community VLANs. Layer 3 gateways are typically connected to the switch through a promiscuous port. With a promiscuous port, you can connect a wide range of devices as access points to a private VLAN. For example, you can use a promiscuous port to monitor or back up all the private-VLAN servers from an administration workstation.

In a switched environment, you can assign an individual private VLAN and associated IP subnet to each individual or common group of end stations. The end stations need to communicate only with a default gateway to communicate outside the private VLAN.

You can use private VLANs to control access to end stations in these ways:

- Configure selected interfaces connected to end stations as isolated ports to prevent any communication at Layer 2. For example, if the end stations are servers, this configuration prevents Layer 2 communication between the servers.

- Configure interfaces connected to default gateways and selected end stations (for example, backup servers) as promiscuous ports to allow all end stations access to a default gateway.

You can extend private VLANs across multiple devices by trunking the primary, isolated, and community VLANs to other devices that support private VLANs. To maintain the security of your private-VLAN configuration and to avoid other use of the VLANs configured as private VLANs, configure private VLANs on all intermediate devices, including devices that have no private-VLAN ports.

### IP Addressing Scheme with Private VLANs

Assigning a separate VLAN to each customer creates an inefficient IP addressing scheme:

- Assigning a block of addresses to a customer VLAN can result in unused IP addresses.

- If the number of devices in the VLAN increases, the number of assigned addresses might not be large enough to accommodate them.

These problems are reduced by using private VLANs, where all members in the private VLAN share a common address space, which is allocated to the primary VLAN. Hosts are connected to secondary VLANs, and the DHCP server assigns them IP addresses from the block of addresses allocated to the primary VLAN. Subsequent IP addresses can be assigned to customer devices in different secondary VLANs, but in the same primary VLAN. When new devices are added, the DHCP server assigns them the next available address from a large pool of subnet addresses.
Private VLANs across Multiple Switches

As with regular VLANs, private VLANs can span multiple switches. A trunk port carries the primary VLAN and secondary VLANs to a neighboring switch. The trunk port treats the private VLAN as any other VLAN. A feature of private VLANs across multiple switches is that traffic from an isolated port in switch A does not reach an isolated port on Switch B. See Figure 13-2.

![Private VLANs across Switches](image)

**Figure 13-2** Private VLANs across Switches

VLAN 100 = Primary VLAN
VLAN 201 = Secondary isolated VLAN
VLAN 202 = Secondary community VLAN

Carries VLAN 100, 201, and 202 traffic

Note that for private VLANs to operate correctly between two switches, you must configure VLAN translation on both sides of the trunk. We recommend that you configure VLAN translation on the enhanced-services (ES) port of each switch and use the same private VLAN IDs on the customer ports of both switches. This allows data to pass between the private VLAN end users.

Because VTP does not support private VLANs, you must manually configure private VLANs on all switches in the Layer 2 network. If you do not configure the primary and secondary VLAN associations in some switches in the network, the Layer 2 databases in these switches are not merged. This can result in unnecessary flooding of private-VLAN traffic on those switches.

**Note**

When configuring private VLANs on the switch, always use the default Switch Database Management (SDM) template to balance system resources between unicast routes and Layer 2 entries. If another SDM template is configured, use the `sdm prefer default` global configuration command to set the default template. See Chapter 6, “Configuring SDM Templates.”
Private-VLAN Interaction with Other Features

Private VLANs have specific interaction with some other features, described in these sections:

- Private VLANs and Unicast, Broadcast, and Multicast Traffic, page 13-5
- Private VLANs and SVIs, page 13-5

You should also see the “Secondary and Primary VLAN Configuration” section on page 13-7 under the “Private-VLAN Configuration Guidelines” section.

Private VLANs and Unicast, Broadcast, and Multicast Traffic

In regular VLANs, devices in the same VLAN can communicate with each other at the Layer 2 level, but devices connected to interfaces in different VLANs must communicate at the Layer 3 level. In private VLANs, the promiscuous ports are members of the primary VLAN, while the host ports belong to secondary VLANs. Because the secondary VLAN is associated to the primary VLAN, members of these VLANs can communicate with each other at the Layer 2 level.

In a regular VLAN, broadcasts are forwarded to all ports in that VLAN. Private VLAN broadcast forwarding depends on the port sending the broadcast:

- An isolated port sends a broadcast only to the promiscuous ports or trunk ports.
- A community port sends a broadcast to all promiscuous ports, trunk ports, and ports in the same community VLAN.
- A promiscuous port sends a broadcast to all ports in the private VLAN (other promiscuous ports, trunk ports, isolated ports, and community ports).

Multicast traffic is routed or bridged across private-VLAN boundaries and within a single community VLAN. Multicast traffic is not forwarded between ports in the same isolated VLAN or between ports in different secondary VLANs.

Private VLANs and SVIs

In a Layer 3 switch, a switch virtual interface (SVI) represents the Layer 3 interface of a VLAN. Layer 3 devices communicate with a private VLAN only through the primary VLAN and not through secondary VLANs. Configure Layer 3 VLAN interfaces only for primary VLANs. You cannot configure Layer 3 VLAN interfaces for secondary VLANs. SVIs for secondary VLANs are inactive while the VLAN is configured as a secondary VLAN.

- If you try to configure a VLAN with an active SVI as a secondary VLAN, the configuration is not allowed until you disable the SVI.
- If you try to create an SVI on a VLAN that is configured as a secondary VLAN and the secondary VLAN is already mapped at Layer 3, the SVI is not created, and an error is returned. If the SVI is not mapped at Layer 3, the SVI is created, but it is automatically shut down.

When the primary VLAN is associated with and mapped to the secondary VLAN, any configuration on the primary VLAN is propagated to the secondary VLAN SVIs. For example, if you assign an IP subnet to the primary VLAN SVI, this subnet is the IP subnet address of the entire private VLAN.
Configuring Private VLANs

This section includes guidelines and procedures for configuring private VLANs. These sections are included:

- Tasks for Configuring Private VLANs, page 13-6
- Default Private-VLAN Configuration, page 13-6
- Private-VLAN Configuration Guidelines, page 13-7
- Configuring and Associating VLANs in a Private VLAN, page 13-10
- Configuring a Layer 2 Interface as a Private-VLAN Host Port, page 13-11
- Configuring a Layer 2 Interface as a Private-VLAN Promiscuous Port, page 13-12
- Mapping Secondary VLANs to a Primary VLAN Layer 3 VLAN Interface, page 13-13

Tasks for Configuring Private VLANs

To configure a private VLAN, follow these steps:

- **Step 1** Set VTP mode to transparent.
- **Step 2** Create the primary and secondary VLANs and associate them. See the “Configuring and Associating VLANs in a Private VLAN” section on page 13-10.
- **Note** If the VLAN is not created already, the private-VLAN configuration process creates it.
- **Step 3** Configure interfaces to be isolated or community host ports, and assign VLAN membership to the host port. See the “Configuring a Layer 2 Interface as a Private-VLAN Host Port” section on page 13-11.
- **Step 4** Configure interfaces as promiscuous ports, and map the promiscuous ports to the primary-secondary VLAN pair. See the “Configuring a Layer 2 Interface as a Private-VLAN Promiscuous Port” section on page 13-12.
- **Step 5** If inter-VLAN routing will be used, configure the primary SVI, and map secondary VLANs to the primary. See the “Mapping Secondary VLANs to a Primary VLAN Layer 3 VLAN Interface” section on page 13-13.
- **Step 6** Verify private-VLAN configuration.

Default Private-VLAN Configuration

No private VLANs are configured.
Private-VLAN Configuration Guidelines

Guidelines for configuring private VLANs fall into these categories:

- Secondary and Primary VLAN Configuration, page 13-7
- Private-VLAN Port Configuration, page 13-8
- Limitations with Other Features, page 13-9

Secondary and Primary VLAN Configuration

Follow these guidelines when configuring private VLANs:

- If the switch is running VTP version 1 or 2, you must set VTP to transparent mode. After you configure a private VLAN, you should not change the VTP mode to client or server. For information about VTP, see Chapter 12, “Configuring VTP.”

- With VTP version 1 or 2, after you have configured private VLANs, use the `copy running-config startup config` privileged EXEC command to save the VTP transparent mode configuration and private-VLAN configuration in the switch startup configuration file. Otherwise, if the switch resets, it defaults to VTP server mode, which does not support private VLANs. VTP version 3 does support private VLANs.

- VTP version 1 and 2 do not propagate private-VLAN configuration. You must configure private VLANs on each device where you want private-VLAN ports unless the devices are running VTP version 3.

- You cannot configure VLAN 1 or VLANs 1002 to 1005 as primary or secondary VLANs. Extended VLANs (VLAN IDs 1006 to 4094) can belong to private VLANs.

- A primary VLAN can have one isolated VLAN and multiple community VLANs associated with it. An isolated or community VLAN can have only one primary VLAN associated with it.

- Although a private VLAN contains more than one VLAN, only one Spanning Tree Protocol (STP) instance runs for the entire private VLAN. When a secondary VLAN is associated with the primary VLAN, the STP parameters of the primary VLAN are propagated to the secondary VLAN.

- You can enable DHCP snooping on private VLANs. When you enable DHCP snooping on the primary VLAN, it is propagated to the secondary VLANs. If you configure DHCP on a secondary VLAN, the configuration does not take effect if the primary VLAN is already configured.

- When you enable IP source guard on private-VLAN ports, you must enable DHCP snooping on the primary VLAN.

- We recommend that you prune the private VLANs from the trunks on devices that carry no traffic in the private VLANs.

- You can apply different quality of service (QoS) configurations to primary, isolated, and community VLANs.

- Sticky ARP
  - Sticky ARP entries are those learned on SVIs and Layer 3 interfaces. They entries do not age out.
  - The `ip sticky-arp` global configuration command is supported only on SVIs belonging to private VLANs.
- The `ip sticky-arp` interface configuration command is only supported on
  - Layer 3 interfaces
  - SVIs belonging to normal VLANs
  - SVIs belonging to private VLANs

For more information about using the `ip sticky-arp global` configuration and the `ip sticky-arp interface` configuration commands, see the command reference for this release.

- You can configure VLAN maps on primary and secondary VLANs (see the “Configuring VLAN Maps” section on page 33-29). However, we recommend that you configure the same VLAN maps on private-VLAN primary and secondary VLANs.

- When a frame is forwarded through Layer-2 within a private VLAN, the same VLAN map is applied at the ingress side and at the egress side. When a frame is routed from inside a private VLAN to an external port, the private-VLAN map is applied at the ingress side.
  - For frames going upstream from a host port to a promiscuous port, the VLAN map configured on the secondary VLAN is applied.
  - For frames going downstream from a promiscuous port to a host port, the VLAN map configured on the primary VLAN is applied.

To filter out specific IP traffic for a private VLAN, you should apply the VLAN map to both the primary and secondary VLANs.

- To allow data to pass between two private VLANs through a tunnel, configure VLAN translation on the ES ports of the edge switches and use the same VLAN ID on the private VLAN ports of the switches.

- You can apply router ACLs only on the primary-VLAN SVIs. The ACL is applied to both primary and secondary VLAN Layer 3 traffic.

- Although private VLANs provide host isolation at Layer 2, hosts can communicate with each other at Layer 3.

- Private VLANs support these Switched Port Analyzer (SPAN) features:
  - You can configure a private-VLAN port as a SPAN source port.
  - You can use VLAN-based SPAN (VSPAN) on primary, isolated, and community VLANs or use SPAN on only one VLAN to separately monitor egress or ingress traffic.

**Private-VLAN Port Configuration**

Follow these guidelines when configuring private-VLAN ports:

- Use only the private-VLAN configuration commands to assign ports to primary, isolated, or community VLANs. Layer 2 access ports assigned to the VLANs that you configure as primary, isolated, or community VLANs are inactive while the VLAN is part of the private-VLAN configuration. Layer 2 trunk interfaces remain in the STP forwarding state.

- Do not configure ports that belong to a PAgP or LACP EtherChannel as private-VLAN ports. While a port is part of the private-VLAN configuration, any EtherChannel configuration for it is inactive.

- Enable Port Fast and BPDU guard on isolated and community host ports to prevent STP loops due to misconfigurations and to speed up STP convergence (see Chapter 18, “Configuring Optional Spanning-Tree Features”). When enabled, STP applies the BPDU guard feature to all Port Fast-configured Layer 2 LAN ports. Do not enable Port Fast and BPDU guard on promiscuous ports.
• If you delete a VLAN used in the private-VLAN configuration, the private-VLAN ports associated with the VLAN become inactive.
• Private-VLAN ports can be on different network devices if the devices are trunk-connected and the primary and secondary VLANs have not been removed from the trunk.

Limitations with Other Features

When configuring private VLANs, remember these limitations with other features:

- Do not configure fallback bridging on switches with private VLANs.
- When IGMP snooping is enabled on the switch (the default), the switch supports no more than 20 private-VLAN domains.
- Do not configure a remote SPAN (RSPAN) VLAN as a private-VLAN primary or secondary VLAN. For more information about SPAN, see Chapter 28, “Configuring SPAN and RSPAN.”
- Do not configure private-VLAN ports on interfaces configured for these other features:
  - dynamic-access port VLAN membership
  - Dynamic Trunking Protocol (DTP)
  - Port Aggregation Protocol (PAgP)
  - Link Aggregation Control Protocol (LACP)
  - Multicast VLAN Registration (MVR)
  - voice VLAN
- You can configure IEEE 802.1x port-based authentication on a private-VLAN port, but do not configure 802.1x with port security, voice VLAN, or per-user ACL on private-VLAN ports.
- A private-VLAN host or promiscuous port cannot be a SPAN destination port. If you configure a SPAN destination port as a private-VLAN port, the port becomes inactive.
- If you configure a static MAC address on a promiscuous port in the primary VLAN, you must add the same static address to all associated secondary VLANs. If you configure a static MAC address on a host port in a secondary VLAN, you must add the same static MAC address to the associated primary VLAN. When you delete a static MAC address from a private-VLAN port, you must remove all instances of the configured MAC address from the private VLAN.

- Dynamic MAC addresses learned in one VLAN of a private VLAN are replicated in the associated VLANs. For example, a MAC address learned in a secondary VLAN is replicated in the primary VLAN. When the original dynamic MAC address is deleted or aged out, the replicated addresses are removed from the MAC address table.

- Configure Layer 3 VLAN interfaces only for primary VLANs.
Chapter 13  Configuring Private VLANs

Configuring and Associating VLANs in a Private VLAN

Beginning in privileged EXEC mode, follow these steps to configure a private VLAN:

Note

The private-vlan commands do not take effect until you exit VLAN configuration mode.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 vtp mode transparent</td>
<td>Set VTP mode to transparent (disable VTP).</td>
</tr>
<tr>
<td>Step 3 vlan vlan-id</td>
<td>Enter VLAN configuration mode and designate or create a VLAN that will be the primary VLAN. The VLAN ID range is 2 to 1001 and 1006 to 4094.</td>
</tr>
<tr>
<td>Step 4 private-vlan primary</td>
<td>Designate the VLAN as the primary VLAN.</td>
</tr>
<tr>
<td>Step 5 exit</td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td>Step 6 vlan vlan-id</td>
<td>(Optional) Enter VLAN configuration mode and designate or create a VLAN that will be an isolated VLAN. The VLAN ID range is 2 to 1001 and 1006 to 4094.</td>
</tr>
<tr>
<td>Step 7 private-vlan isolated</td>
<td>Designate the VLAN as an isolated VLAN.</td>
</tr>
<tr>
<td>Step 8 exit</td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td>Step 9 vlan vlan-id</td>
<td>(Optional) Enter VLAN configuration mode and designate or create a VLAN that will be a community VLAN. The VLAN ID range is 2 to 1001 and 1006 to 4094.</td>
</tr>
<tr>
<td>Step 10 private-vlan community</td>
<td>Designate the VLAN as a community VLAN.</td>
</tr>
<tr>
<td>Step 11 exit</td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td>Step 12 vlan vlan-id</td>
<td>Enter VLAN configuration mode for the primary VLAN designated in Step 2.</td>
</tr>
<tr>
<td>Step 13 private-vlan association [add</td>
<td>remove] secondary_vlan_list</td>
</tr>
<tr>
<td>Step 14 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 15 show vlan private-vlan [type] or show interfaces status</td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td>Step 16 copy running-config startup config</td>
<td>Save your entries in the switch startup configuration file. To save the private-VLAN configuration, you need to save the VTP transparent mode configuration and private-VLAN configuration in the switch startup configuration file. Otherwise, if the switch resets, it defaults to VTP server mode, which does not support private VLANs.</td>
</tr>
</tbody>
</table>

When you associate secondary VLANs with a primary VLAN, note this syntax information:

- The secondary_vlan_list parameter cannot contain spaces. It can contain multiple comma-separated items. Each item can be a single private-VLAN ID or a hyphenated range of private-VLAN IDs.
The **secondary_vlan_list** parameter can contain multiple community VLAN IDs but only one isolated VLAN ID.

- Enter a **secondary_vlan_list**, or use the **add** keyword with a **secondary_vlan_list** to associate secondary VLANs with a primary VLAN.
- Use the **remove** keyword with a **secondary_vlan_list** to clear the association between secondary VLANs and a primary VLAN.
- The command does not take effect until you exit VLAN configuration mode.

This example shows how to configure VLAN 20 as a primary VLAN, VLAN 501 as an isolated VLAN, and VLANs 502 and 503 as community VLANs, to associate them in a private VLAN, and to verify the configuration:

```
Switch# configure terminal
Switch(config)# vlan 20
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# exit
Switch(config)# vlan 501
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# exit
Switch(config)# vlan 502
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# exit
Switch(config)# vlan 503
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# exit
Switch(config)# vlan 20
Switch(config-vlan)# private-vlan association 501-503
Switch(config-vlan)# end
Switch(config)# show vlan private vlan
```

<table>
<thead>
<tr>
<th>Primary</th>
<th>Secondary</th>
<th>Type</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>501</td>
<td>isolated</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>502</td>
<td>community</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>503</td>
<td>community</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>504</td>
<td>non-operational</td>
<td></td>
</tr>
</tbody>
</table>

**Configuring a Layer 2 Interface as a Private-VLAN Host Port**

Beginning in privileged EXEC mode, follow these steps to configure a Layer 2 interface as a private-VLAN host port and to associate it with primary and secondary VLANs:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> interface interface-id</td>
<td>Enter interface configuration mode for the Layer 2 interface to be configured.</td>
</tr>
<tr>
<td><strong>Step 3</strong> switchport mode private-vlan host</td>
<td>Configure the Layer 2 port as a private-VLAN host port.</td>
</tr>
<tr>
<td><strong>Step 4</strong> switchport private-vlan host-association</td>
<td>Associate the Layer 2 port with a private VLAN.</td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

---

**Note**

Isolated and community VLANs are both secondary VLANs.
Chapter 13 Configuring Private VLANs

Configuring Private VLANs

This example shows how to configure an interface as a private-VLAN host port, associate it with a private-VLAN pair, and verify the configuration:

```
Switch# configure terminal
Switch(config)# interface fastethernet 1/0/22
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 20 501
Switch(config-if)# end
Switch#
```

```
show interfaces fastethernet 1/0/22 switchport
```

### Configuring a Layer 2 Interface as a Private-VLAN Promiscuous Port

Beginning in privileged EXEC mode, follow these steps to configure a Layer 2 interface as a private-VLAN promiscuous port and map it to primary and secondary VLANs:

1. **configure terminal**
   - Enter global configuration mode.

2. **interface interface-id**
   - Enter interface configuration mode for the Layer 2 interface to be configured.

3. **switchport mode private-vlan promiscuous**
   - Configure the Layer 2 port as a private-VLAN promiscuous port.

---

**Note**

Isolated and community VLANs are both secondary VLANs.

---

### Command Purpose

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show interfaces [interface-id] switchport</td>
<td>Verify the configuration.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 7</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>copy running-config startup config</td>
<td>(Optional) Save your entries in the switch startup configuration file.</td>
<td></td>
</tr>
</tbody>
</table>
When you configure a Layer 2 interface as a private-VLAN promiscuous port, note this syntax information:

- The `secondary_vlan_list` parameter cannot contain spaces. It can contain multiple comma-separated items. Each item can be a single private-VLAN ID or a hyphenated range of private-VLAN IDs.
- Enter a `secondary_vlan_list`, or use the `add` keyword with a `secondary_vlan_list` to map the secondary VLANs to the private-VLAN promiscuous port.
- Use the `remove` keyword with a `secondary_vlan_list` to clear the mapping between secondary VLANs and the private-VLAN promiscuous port.

This example shows how to configure an interface as a private-VLAN promiscuous port and map it to a private VLAN. The interface is a member of primary VLAN 20 and secondary VLANs 501 to 503 are mapped to it.

```
Switch# configure terminal
Switch(config)# interface fastethernet 1/0/2
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan mapping 20 add 501-503
Switch(config-if)# end
```

Use the `show vlan private-vlan` or the `show interface status` privileged EXEC command to display primary and secondary VLANs and private-VLAN ports on the switch.

### Mapping Secondary VLANs to a Primary VLAN Layer 3 VLAN Interface

If the private VLAN will be used for inter-VLAN routing, you configure an SVI for the primary VLAN and map secondary VLANs to the SVI.

**Note**

Isolated and community VLANs are both secondary VLANs.

Beginning in privileged EXEC mode, follow these steps to map secondary VLANs to the SVI of a primary VLAN to allow Layer 3 switching of private-VLAN traffic:

```
Command | Purpose
--- | ---
Step 1 configure terminal | Enter global configuration mode.
Step 2 interface vlan primary_vlan_id | Enter interface configuration mode for the primary VLAN, and configure the VLAN as an SVI. The VLAN ID range is 2 to 1001 and 1006 to 4094.
```
Chapter 13      Configuring Private VLANs

Monitoring Private VLANs

Table 13-1 shows the privileged EXEC commands for monitoring private-VLAN activity.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show interfaces status</td>
<td>Displays the status of interfaces, including the VLANs to which they belong.</td>
</tr>
<tr>
<td>show vlan private-vlan [type]</td>
<td>Display the private-VLAN information for the switch.</td>
</tr>
</tbody>
</table>

**Note** The `private-vlan mapping` interface configuration command only affects private-VLAN traffic that is switched through Layer 3.

When you map secondary VLANs to the Layer 3 VLAN interface of a primary VLAN, note this syntax information:

- The `secondary_vlan_list` parameter cannot contain spaces. It can contain multiple comma-separated items. Each item can be a single private-VLAN ID or a hyphenated range of private-VLAN IDs.
- Enter a `secondary_vlan_list`, or use the `add` keyword with a `secondary_vlan_list` to map the secondary VLANs to the primary VLAN.
- Use the `remove` keyword with a `secondary_vlan_list` to clear the mapping between secondary VLANs and the primary VLAN.

This example shows how to map the interfaces of VLANs 501 and 502 to primary VLAN 10, which permits routing of secondary VLAN ingress traffic from private VLANs 501 to 502:

```
Switch# configure terminal
Switch(config)# interface vlan 10
Switch(config-if)# private-vlan mapping 501-502
Switch(config-if)# end
Switch# show interfaces private-vlan mapping
Interface Secondary VLAN Type
---------- ----------------- --------------
vlan10     501            isolated
vlan10     502            community
```
**Table 13-1  Private VLAN Monitoring Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show interface switchport</td>
<td>Display the private-VLAN configuration on interfaces.</td>
</tr>
<tr>
<td>show interface private-vlan mapping</td>
<td>Display information about the private-VLAN mapping for VLAN SVIs.</td>
</tr>
</tbody>
</table>

This is an example of the output from the **show vlan private-vlan** command:

```
Switch(config)# show vlan private-vlan
Primary Secondary Type               Ports
------- --------- ----------------- ------------------------------------------
10      501       isolated          Fa1/0/1, Gi1/0/1, Gi1/0/2
10      502       community         Fa1/0/11, Gi1/0/1, Gi1/0/4
10      503       non-operational
```
Configuring Voice VLAN

This chapter describes how to configure the voice VLAN feature on the Catalyst 3750 Metro switch. Voice VLAN is also referred to as an auxiliary VLAN in some Catalyst 6500 family switch documentation.

Note

For complete syntax and usage information for the commands used in this chapter, see the command reference for this release.

This chapter consists of these sections:

- Understanding Voice VLAN, page 14-1
- Configuring Voice VLAN, page 14-3
- Displaying Voice VLAN, page 14-6

Understanding Voice VLAN

The voice VLAN feature enables access ports to carry IP voice traffic from an IP phone. When the switch is connected to a Cisco 7960 IP Phone, the IP Phone sends voice traffic with Layer 3 IP precedence and Layer 2 class of service (CoS) values, which are both set to 5 by default. Because the sound quality of an IP phone call can deteriorate if the data is unevenly sent, the switch supports quality of service (QoS) based on IEEE 802.1p CoS. QoS uses classification and scheduling to send network traffic from the switch in a predictable manner. For more information on QoS, see Chapter 34, “Configuring QoS.”

The Cisco 7960 IP Phone is a configurable device, and you can configure it to forward traffic with an 802.1p priority. You can configure the switch to trust or override the traffic priority assigned by an IP Phone.

The Cisco IP Phone contains an integrated three-port 10/100 switch as shown in Figure 14-1. The ports provide dedicated connections to these devices:

- Port 1 connects to the switch or other voice-over-IP (VoIP) device.
- Port 2 is an internal 10/100 interface that carries the IP phone traffic.
- Port 3 (access port) connects to a PC or other device.

Figure 14-1 shows one way to connect a Cisco 7960 IP Phone.
Understanding Voice VLAN

Cisco IP Phone Voice Traffic

You can configure an access port with an attached Cisco IP Phone to use one VLAN for voice traffic and another VLAN for data traffic from a device attached to the phone. You can configure access ports on the switch to send Cisco Discovery Protocol (CDP) packets that instruct an attached Cisco IP Phone to send voice traffic to the switch in any of these ways:

- In the voice VLAN tagged with a Layer 2 CoS priority value
- In the access VLAN tagged with a Layer 2 CoS priority value
- In the access VLAN, untagged (no Layer 2 CoS priority value)

**Note**
In all configurations, the voice traffic carries a Layer 3 IP precedence value (the default is 5 for voice traffic and 3 for voice control traffic).

Cisco IP Phone Data Traffic

The switch can also process tagged data traffic (traffic in 802.1Q or 802.1p frame types) from the device attached to the access port on the Cisco IP Phone (see Figure 14-1). You can configure Layer 2 access ports on the switch to send CDP packets that instruct the attached Cisco IP Phone to configure the IP phone access port in one of these modes:

- In trusted mode, all traffic received through the access port on the Cisco IP Phone passes through the IP phone unchanged.
- In untrusted mode, all traffic in 802.1Q or 802.1p frames received through the access port on the IP phone receive a configured Layer 2 CoS value. The default Layer 2 CoS value is 0. Untrusted mode is the default.

**Note**
Untagged traffic from the device attached to the Cisco IP Phone passes through the IP phone unchanged, regardless of the trust state of the access port on the IP phone.
Configuring Voice VLAN

This section describes how to configure voice VLAN on access ports. This section contains this configuration information:

- Default Voice VLAN Configuration, page 14-3
- Voice VLAN Configuration Guidelines, page 14-3
- Configuring a Port Connected to a Cisco 7960 IP Phone, page 14-4

Default Voice VLAN Configuration

The voice VLAN feature is disabled by default.

When the voice VLAN feature is enabled, all untagged traffic is sent according to the default CoS priority of the port.

The CoS value is not trusted for 802.1p or 802.1Q tagged traffic.

Voice VLAN Configuration Guidelines

These are the voice VLAN configuration guidelines:

- Voice VLAN configuration is only supported on switch access ports; voice VLAN configuration is not supported on trunk ports.

Trunk ports can carry any number of voice VLANs, similar to regular VLANs. The configuration of voice VLANs is not required on trunk ports.

- Do not configure voice VLAN on private VLAN ports.
- Before you enable voice VLAN, we recommend that you enable QoS on the switch by entering the `mls qos` global configuration command and configure the port trust state to trust by entering the `mls qos trust cos` interface configuration command. If you use the auto-QoS feature, these settings are automatically configured. For more information, see Chapter 34, “Configuring QoS.”
- You must enable CDP on the switch port connected to the Cisco IP Phone to send configuration to the Cisco IP Phone. (CDP is enabled by default globally and on all switch interfaces.)
- The Port Fast feature is automatically enabled when voice VLAN is configured. When you disable voice VLAN, the Port Fast feature is not automatically disabled.
- If the Cisco IP Phone and a device attached to the Cisco IP Phone are in the same VLAN, they must be in the same IP subnet. These conditions indicate that they are in the same VLAN:
  - They both use 802.1p or untagged frames.
  - The Cisco IP Phone uses 802.1p frames and the device uses untagged frames.
  - The Cisco IP Phone uses untagged frames and the device uses 802.1p frames.
  - The Cisco IP Phone uses 802.1Q frames and the voice VLAN is the same as the access VLAN.
- The Cisco IP Phone and a device attached to the phone cannot communicate if they are in the same VLAN and subnet but use different frame types because traffic in the same subnet is not routed (routing would eliminate the frame type difference).
You cannot configure static secure MAC addresses in the voice VLAN.

Voice VLAN ports can also be these port types:

- Dynamic access port. See the “Configuring Dynamic-Access Ports on VMPS Clients” section on page 11-30 for more information.
- 802.1X authenticated port. See the “Configuring IEEE 802.1x Authentication” section on page 8-14 for more information.
- Protected port. See the “Configuring Protected Ports” section on page 24-6 for more information.
- A source or destination port for a SPAN or RSPAN session.
- Secure port. See the “Configuring Port Security” section on page 24-8 for more information.

Note When you enable port security on an interface that is also configured with a voice VLAN, you must set the maximum allowed secure addresses on the port to two plus the maximum number of secure addresses allowed on the access VLAN. When the port is connected to a Cisco IP phone, the IP phone requires up to two MAC addresses. The IP phone address is learned on the voice VLAN and might also be learned on the access VLAN. Connecting a PC to the IP phone requires additional MAC addresses.

Configuring a Port Connected to a Cisco 7960 IP Phone

Because a Cisco 7960 IP Phone also supports a connection to a PC or other device, a port connecting the switch to a Cisco IP Phone can carry mixed traffic. You can configure a port to determine how the IP phone carries voice traffic and data traffic.

This section includes these topics:

- Configuring IP Phone Voice Traffic, page 14-4
- Configuring the Priority of Incoming Data Frames, page 14-5

Configuring IP Phone Voice Traffic

You can configure a port connected to the Cisco IP Phone to send CDP packets to the phone to configure the way in which the phone sends voice traffic. The phone can carry voice traffic in 802.1Q frames for a specified voice VLAN with a Layer 2 CoS value. It can use 802.1P priority tagging to give voice traffic a higher priority and forward all voice traffic through the native (access) VLAN. The IP phone can also send untagged voice traffic or use its own configuration to send voice traffic in the access VLAN. In all configurations, the voice traffic carries a Layer 3 IP precedence value (the default is 5).

Beginning in privileged EXEC mode, follow these steps to configure voice traffic on a port:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>interface interface-id</td>
<td>Enter interface configuration mode, and specify the interface connected to the IP phone.</td>
</tr>
</tbody>
</table>
### Chapter 14 Configuring Voice VLAN

#### Configuring Voice VLAN

This example shows how to configure a port connected to an IP phone to use the CoS value to classify ingress traffic, to use 802.1P priority tagging for voice traffic, and to use the default native VLAN (VLAN 0) to carry all traffic:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 3**<br>mls qos trust cos | Configure the interface to classify ingress traffic packets by using the packet CoS value. For untagged packets, the port default CoS value is used.  
**Note** Before configuring the port trust state, you must first globally enable QoS by using the `mls qos` global configuration command. |
| **Step 4**<br>switchport voice vlan {vlan-id | dot1p | none | untagged} | Configure how the Cisco IP Phone carries voice traffic:  
- **vlan-id**—Configure the Cisco IP Phone to forward all voice traffic through the specified VLAN. By default, the Cisco IP Phone forwards the voice traffic with an 802.1Q priority of 5. Valid VLAN IDs are from 1 to 4094.  
- **dot1p**—Configure the Cisco IP Phone to use 802.1P priority tagging for voice traffic and to use the default native VLAN (VLAN 0) to carry all traffic. By default, the Cisco IP Phone forwards the voice traffic with an 802.1P priority of 5.  
- **none**—Allow the IP phone to use its own configuration to send untagged voice traffic.  
- **untagged**—Configure the phone to send untagged voice traffic. |
| **Step 5**<br>end | Return to privileged EXEC mode. |
| **Step 6**<br>show interfaces interface-id switchport or show running-config interface interface-id | Verify your voice VLAN entries. Verify your QoS and voice VLAN entries. |
| **Step 7**<br>copy running-config startup-config | (Optional) Save your entries in the configuration file. |

This example shows how to configure a port connected to an IP phone to use the CoS value to classify ingress traffic, to use 802.1P priority tagging for voice traffic, and to use and the default native VLAN (VLAN 0) to carry all traffic:

```
Switch# configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Switch(config)# interface gigabitethernet1/0/1  
Switch(config-if)# mls qos trust cos  
Switch(config-if)# switchport voice vlan dot1p  
Switch(config-if)# end  
```

To return the port to its default setting, use the `no switchport voice vlan` interface configuration command.

### Configuring the Priority of Incoming Data Frames

You can connect a PC or other data device to a Cisco IP Phone port. To process tagged data traffic (in 802.1Q or 802.1P frames), you can configure the switch to send CDP packets to instruct the IP phone how to send data packets from the device attached to the access port on the Cisco IP Phone. The PC can generate packets with an assigned CoS value. You can configure the Cisco IP Phone to not change (trust) or to override (not trust) the priority of frames arriving on the IP phone port from connected devices.
Beginning in privileged EXEC mode, follow these steps to set the priority of data traffic received from
the nonvoice port on the Cisco IP Phone:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Enter interface configuration mode, and specify the interface connected to the IP phone.</td>
</tr>
<tr>
<td>Step 3 switchport priority extend</td>
<td>Set the priority of data traffic received from the IP phone access port:</td>
</tr>
<tr>
<td>{ cos value</td>
<td>trust }</td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5 show interfaces interface-id switchport</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 6 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

This example shows how to configure a port connected to an IP phone to not change the priority of frames received from the PC or the attached device:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# switchport priority extend trust
Switch(config-if)# end
```

To return the port to its default setting, use the no switchport priority extend interface configuration command.

**Displaying Voice VLAN**

To display voice VLAN configuration for an interface, use the show interfaces interface-id switchport privileged EXEC command.
Configuring IEEE 802.1Q and Layer 2 Protocol Tunneling

Virtual private networks (VPNs) provide enterprise-scale connectivity on a shared infrastructure, often Ethernet-based, with the same security, prioritization, reliability, and manageability requirements of private networks. Tunneling is a feature designed for service providers who carry traffic of multiple customers across their networks and are required to maintain the VLAN and Layer 2 protocol configurations of each customer without impacting the traffic of other customers. The Catalyst 3750 Metro switch supports IEEE 802.1Q tunneling and Layer 2 protocol tunneling, as well as VLAN mapping (VLAN-ID translation).

Note

For complete syntax and usage information for the commands used in this chapter, see the command reference for this release.

This chapter contains these sections:
- Understanding IEEE 802.1Q Tunneling, page 15-1
- Configuring IEEE 802.1Q Tunneling, page 15-4
- Configuring VLAN Mapping, page 15-7
- Configuring IEEE 802.1ad, page 15-11
- Understanding Layer 2 Protocol Tunneling, page 15-17
- Configuring Layer 2 Protocol Tunneling, page 15-19
- Monitoring and Maintaining Tunneling and Mapping Status, page 15-27

Note

For information about VPNs used with multiprotocol label switching (MPLS), see Chapter 44, “Configuring MPLS, MPLS VPN, MPLS OAM, and EoMPLS.”

Understanding IEEE 802.1Q Tunneling

Service-provider business customers often have specific requirements for VLAN IDs and the number of VLANs to be supported. The VLAN ranges required by different customers in the same service-provider network might overlap, and traffic of customers through the infrastructure might be mixed. Assigning a unique range of VLAN IDs to each customer would restrict customer configurations and could easily exceed the VLAN limit (4096) of the IEEE 802.1Q specification.
Understanding IEEE 802.1Q Tunneling

Using the IEEE 802.1Q tunneling feature, service providers can use a single VLAN to support customers who have multiple VLANs. Customer VLAN IDs are preserved, and traffic from different customers is segregated within the service-provider infrastructure, even when they appear to be on the same VLAN. Using IEEE 802.1Q tunneling expands VLAN space by using a VLAN-in-VLAN hierarchy and tagging the tagged packets. A port configured to support IEEE 802.1Q tunneling is called a *tunnel port*. When you configure tunneling, you assign a tunnel port to a VLAN that is dedicated to tunneling. Each customer requires a separate service-provider VLAN ID, but that VLAN ID supports all of the customer’s VLANs.

Customer traffic tagged in the normal way with appropriate VLAN IDs come from an IEEE 802.1Q trunk port on the customer device and into a tunnel port on the service-provider edge switch. The link between the customer device and the edge switch is an asymmetric link because one end is configured as an IEEE 802.1Q trunk port and the other end is configured as a tunnel port. You assign the tunnel port interface to an access VLAN ID that is unique to each customer. See Figure 15-1.

![Figure 15-1 IEEE 802.1Q Tunnel Ports in a Service-Provider Network](image)

Packets coming from the customer trunk port into the tunnel port on the service-provider edge switch are normally IEEE 802.1Q-tagged with the appropriate VLAN ID. The tagged packets remain intact inside the switch and, when they exit the trunk port into the service-provider network, are encapsulated with another layer of an IEEE 802.1Q tag (called the *metro tag*) that contains the VLAN ID that is unique to the customer. The original IEEE 802.1Q tag from the customer is preserved in the encapsulated packet. Therefore, packets entering the service-provider infrastructure are double-tagged, with the outer tag containing the customer’s access VLAN ID, and the inner VLAN ID being the VLAN of the incoming traffic.

When the double-tagged packet enters another trunk port in a service-provider core switch, the outer tag is stripped as the packet is processed inside the switch. When the packet exits another trunk port on the same core switch, the same metro tag is again added to the packet. Figure 15-2 shows the structure of the double-tagged packet.
When the packet enters the trunk port of the service-provider egress switch, the outer tag is again stripped as the packet is processed internally on the switch. However, the metro tag is not added when it is sent out the tunnel port on the edge switch into the customer network, and the packet is sent as a normal IEEE 802.1Q-tagged frame to preserve the original VLAN numbers in the customer network.

In Figure 15-1, Customer A was assigned VLAN 30, and Customer B was assigned VLAN 40. Packets entering the edge-switch tunnel ports with IEEE 802.1Q tags are double-tagged when they enter the service-provider network, with the outer tag containing VLAN ID 30 or 40, appropriately, and the inner tag containing the original VLAN number, for example, VLAN 100. Even if both Customers A and B have VLAN 100 in their networks, the traffic remains segregated within the service-provider network because the outer tag is different. With IEEE 802.1Q tunneling, each customer controls its own VLAN numbering space, which is independent of the VLAN numbering space used by other customers and the VLAN numbering space used by the service-provider network.

At the outbound tunnel port, the original VLAN numbers on the customer's network are recovered. It is possible to have multiple levels of tunneling and tagging, but the switch supports only one level in this release.

If the traffic coming from a customer network is not tagged (native VLAN frames), these packets are bridged or routed as if they were normal packets. All packets entering the service-provider network through a tunnel port on an edge switch are treated as untagged packets, whether they are untagged or already tagged with IEEE 802.1Q headers. The packets are encapsulated with the metro tag VLAN ID (set to the access VLAN of the tunnel port) when they are sent through the service-provider network on an IEEE 802.1Q trunk port. The priority field on the metro tag is set to the interface class of service (CoS) priority configured on the tunnel port (the default is zero if none is configured).

The switch supports intelligent IEEE 802.1Q tunneling QoS, or the ability to copy the inner CoS value to the outer CoS value. For more information, see the “Configuring the Trust State on Ports Within the QoS Domain” section on page 34-56 and the “Configuring the CoS Value for an Interface” section on page 34-59.
Configuring IEEE 802.1Q Tunneling

This section includes this information about configuring IEEE 802.1Q tunneling:

- Default IEEE 802.1Q Tunneling Configuration, page 15-4
- IEEE 802.1Q Tunneling Configuration Guidelines, page 15-4
- IEEE 802.1Q Tunneling and Other Features, page 15-6
- Configuring an IEEE 802.1Q Tunneling Port, page 15-6

Default IEEE 802.1Q Tunneling Configuration

By default, IEEE 802.1Q tunneling is disabled because the default switchport mode is dynamic auto. Tagging of IEEE 802.1Q native VLAN packets on all IEEE 802.1Q trunk ports is also disabled.

IEEE 802.1Q Tunneling Configuration Guidelines

When you configure IEEE 802.1Q tunneling (QinQ), you should always use an asymmetrical link between the customer device and the edge switch, with the customer device port configured as an IEEE 802.1Q trunk port and the edge switch port configured as a tunnel port.

Assign tunnel ports only to VLANs that are used for tunneling.

To allow data to pass between two private VLANs through a tunnel, configure VLAN translation on the ES ports of the edge switches and use the same VLAN ID on the private VLAN ports of the switches.

Configuration requirements for native VLANs and maximum transmission units (MTUs) are explained in the next sections.

Note

The switch does not support IPv6 features with any ES-port specific features, such as QinQ trust.

Native VLANs

When configuring IEEE 802.1Q tunneling on an edge switch, you must use IEEE 802.1Q trunk ports for sending out packets into the service-provider network. However, packets going through the core of the service-provider network might be carried through IEEE 802.1Q trunks, ISL trunks, or nontrunking links. When IEEE 802.1Q trunks are used in these core switches, the native VLANs of the IEEE 802.1Q trunks must not match any native VLAN of the nontrunking (tunneling) port on the same switch because traffic on the native VLAN would not be tagged on the IEEE 802.1Q transmitting trunk port.

See Figure 15-3. VLAN 40 is configured as the native VLAN for the IEEE 802.1Q trunk port from Customer X at the ingress edge switch in the service-provider network (Switch B). Switch A of Customer X sends a tagged packet on VLAN 30 to the ingress tunnel port of Switch B in the service-provider network, which belongs to access VLAN 40. Because the access VLAN of the tunnel port (VLAN 40) is the same as the native VLAN of the edge switch trunk port (VLAN 40), the metro tag is not added to tagged packets received from the tunnel port. The packet carries only the VLAN 30 tag through the service-provider network to the trunk port of the egress edge switch (Switch C) and is misdirected through the egress switch tunnel port to Customer Y.
These are some ways to solve this problem:

- Use ISL trunks on standard ports between core switches in the service-provider network. Although customer interfaces connected to edge switches must be IEEE 802.1Q trunks, we recommend using ISL trunks for connecting switches in the core layer.

- Use the `vlan dot1q tag native` global configuration command to configure the edge switch so that all packets going out an IEEE 802.1Q trunk, including the native VLAN, are tagged. If the switch is configured to tag native VLAN packets on all IEEE 802.1Q trunks, the switch accepts untagged packets, but sends only tagged packets.

- Ensure that the native VLAN ID on the edge switch trunk port is not within the customer VLAN range. For example, if the trunk port carries traffic of VLANs 100 to 200, assign the native VLAN a number outside that range.

**Figure 15-3 Potential Problem with IEEE 802.1Q Tunneling and Native VLANs**

---

**System MTU**

The default system MTU for traffic on the Catalyst 3750 Metro switch is 1500 bytes. You can configure Fast Ethernet ports to support frames larger than 1500 bytes by using the `system mtu` global configuration command. You can configure Gigabit Ethernet ports to support frames larger than 1500 bytes by using the `system mtu jumbo` global configuration command. Because the IEEE 802.1Q tunneling feature increases the frame size by 4 bytes when the metro tag is added, you must configure all switches in the service-provider network to be able to process maximum frames by increasing the switch system MTU size to at least 1504 bytes. The maximum allowable system MTU for Gigabit Ethernet interfaces is 9000 bytes; the maximum system MTU for Fast Ethernet interfaces is 1998 bytes.
IEEE 802.1Q Tunneling and Other Features

Although IEEE 802.1Q tunneling works well for Layer 2 packet switching, there are incompatibilities with some Layer 2 features and with Layer 3 switching.

- A tunnel port cannot be a routed port.
- IP routing is not supported on a VLAN that includes IEEE 802.1Q ports. Packets received from a tunnel port are forwarded based only on Layer 2 information. If routing is enabled on the switch virtual interface (SVI) that includes tunnel ports, untagged IP packets received from the tunnel port are recognized and routed by the switch. This allows the customer to access the Internet through its native VLAN. If this access is not required, you should not configure SVIs on VLANs that include tunnel ports.
- Fallback bridging is not supported on tunnel ports. Because all IEEE 802.1Q-tagged packets received from a tunnel port are treated as non-IP packets, if fallback bridging is enabled on VLANs that have tunnel ports configured, IP packets would be improperly bridged across VLANs. Therefore, you must not enable fallback bridging on VLANs with tunnel ports.
- Tunnel ports do not support IP access control lists (ACLs).
- Layer 3 quality of service (QoS) ACLs and other QoS features related to Layer 3 information are not supported on tunnel ports. MAC-based QoS ACLs are supported on tunnel ports.
- EtherChannel port groups are compatible with tunnel ports as long as the IEEE 802.1Q configuration is consistent within an EtherChannel port group.
- Port Aggregation Protocol (PAgP), Link Aggregation Control Protocol (LACP), and UniDirectional Link Detection (UDLD) are supported on IEEE 802.1Q tunnel ports.
- Dynamic Trunking Protocol (DTP) is not compatible with IEEE 802.1Q tunneling because you must manually configure asymmetric links with tunnel ports and trunk ports.
- VLAN Trunking Protocol (VTP) does not work between devices that are connected by an asymmetrical link or devices that communicate through a tunnel.
- Loopback detection is supported on IEEE 802.1Q tunnel ports.
- When a port is configured as an IEEE 802.1Q tunnel port, spanning-tree bridge protocol data unit (BPDU) filtering is automatically enabled on the interface. Cisco Discovery Protocol (CDP) and the Layer Link Discovery Protocol (LLDP) are automatically disabled on the interface.

Configuring an IEEE 802.1Q Tunneling Port

Beginning in privileged EXEC mode, follow these steps to configure a port as an IEEE 802.1Q tunnel port:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Enter interface configuration mode and the interface to be configured as a tunnel port. This should be the edge port in the service-provider network that connects to the customer switch. Valid interfaces include physical interfaces and port-channel logical interfaces (port channels 1 to 12).</td>
</tr>
<tr>
<td>Step 3 switchport access vlan vlan-id</td>
<td>Specify the default VLAN, which is used if the interface stops trunking. This VLAN ID is specific to the particular customer.</td>
</tr>
</tbody>
</table>
Use the no switchport mode dot1q-tunnel interface configuration command to return the port to the default state of dynamic auto. Use the no vlan dot1q tag native global configuration command to disable tagging of native VLAN packets.

This example shows how to configure a port as a tunnel port, enable tagging of native VLAN packets, and verify the configuration. In this configuration, the VLAN ID for the customer connected to Fast Ethernet port 7 is VLAN 22.

```
Switch(config)# interface fastethernet1/0/7
Switch(config-if)# switchport access vlan 22
% Access VLAN does not exist. Creating vlan 22
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# exit
Switch(config)# vlan dot1q tag native
Switch(config)# end
Switch# show dot1q-tunnel interface fastethernet1/0/7
Port
-----
Fa1/0/7
-----
Switch# show vlan dot1q tag native
dot1q native vlan tagging is enabled
```

**Configuring VLAN Mapping**

VLAN mapping, or VLAN ID translation, is a feature that you can configure on the enhanced-services (ES) ports connected to the service-provider network to map the customer VLANs to service-provider VLANs. VLAN mapping acts as a filter on the ES ports without affecting the internal operation of the switch or the customer VLANs. A switch might also have a number of reserved VLANs or have a limited VLAN range. When customers want to use a VLAN number in the reserved range, you can use VLAN mapping to overlap customer VLANs by encapsulating the customer traffic in IEEE 802.1Q tunnels.

With VLAN mapping, the customer VLAN ID in the IEEE 802.1Q tag, or the inner and outer tag in an IEEE 802.1Q tunneled frame, are mapped (or translated) just before a packet is transmitted and just after a packet is received. The service-provider VLANs are not seen by the switch, so all configuration and statistics are done with the customer side-VLANs.
The switch supports three types of VLAN mapping:

- One-to-one mapping that maps the customer VLAN ID in the IEEE 802.1Q tag to the service-provider VLAN ID.
- Two-to-one mapping that maps IEEE 802.1Q tunneling traffic with outer and the inner VLAN IDs to the service-provider VLAN ID.
- Two-to-two mapping that maps IEEE 802.1Q tunneling traffic with outer and the inner VLAN IDs to the service-provider outer and the inner VLAN IDs.

The customer-side IEEE 802.1Q VLAN IDs are used to switch the packet inside the switch. The service-provider VLAN IDs are sent or received on the ES ports.

To configure VLAN translation on a port channel of ES ports, enter the `switchport vlan mapping` interface configuration command on each of the ES ports. When configuring the translations at the ES ports, ensure that the VLAN translations are identical on both ES ports.

**Note**

Do not configure VLAN mapping on an interface configured for MPLS or EoMPLS.

This section includes this configuration information:

- Default VLAN Mapping Configuration, page 15-8
- Mapping Customer VLANs to Service-Provider VLANs, page 15-8
- Mapping Customer IEEE 802.1Q Tunnel VLANs to Service-Provider VLANs, page 15-10

### Default VLAN Mapping Configuration

By default, no VLAN mapping is configured.

### Mapping Customer VLANs to Service-Provider VLANs

*Figure 15-4* shows a topology where a customer uses the same VLANs in multiple sites at different sides of a service-provider network. You map the customer VLAN IDs to service-provider VLAN IDs for packet travel across the service-provider backbone. The customer VLAN IDs are retrieved at the other side of the service-provider backbone for use in the other customer site. Configure the same set of VLAN mappings at an ES on each side of the service-provider network. See the example following the configuration steps.
Beginning in privileged EXEC mode, follow these steps on an ES port to map a customer VLAN ID to a service-provider VLAN ID:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> interface interface-id</td>
<td>Enter interface configuration mode and the ES interface connected to the service-provider network.</td>
</tr>
</tbody>
</table>
| **Step 3** switchport vlan mapping vlan-id translated-id | Enter the VLAN IDs to be mapped:  
  - *vlan-id*—the customer VLAN ID entering the switch from the customer network. The range is from 1 to 4094.  
  - *translated-id*—the assigned service-provider VLAN ID. The range is from 1 to 4094. |
| **Step 4** end                 | Return to privileged EXEC mode.      |
| **Step 5** show vlan mapping   | Verify the configuration.            |
| **Step 6** copy running-config startup-config | (Optional) Save your entries in the configuration file. |

Use the no switchport vlan mapping *vlan-id translated-id* command to remove the VLAN translation information.
This example shows how to map VLAN IDs 1, 2, 3, 4, and 5 in the customer network to VLANs 2001, 2002, 2003, and 2004 in the service-provider network as shown in Figure 15-4. You configure these same VLAN mapping commands for an ES port in Switch A and Switch B.

```
Switch(config)# interface gigabiethernet1/1/1
Switch(config-if)# switchport vlan mapping 1 1001
Switch(config-if)# switchport vlan mapping 2 1002
Switch(config-if)# switchport vlan mapping 3 1003
Switch(config-if)# switchport vlan mapping 4 1004
Switch(config-if)# switchport vlan mapping 5 1005
Switch(config-if)# exit
```

In the previous example, at the ingress of the service-provider network, VLAN IDs 1, 2, 3, 4, and 5 in the customer network are mapped to VLANs 2001, 2002, 2003, and 2004 in the service-provider network. At the egress of the service-provider network, VLANs 2001, 2002, 2003, and 2004 in the service-provider network are mapped to VLAN IDs 1, 2, 3, 4, and 5 in the customer network.

### Mapping Customer IEEE 802.1Q Tunnel VLANs to Service-Provider VLANs

You can also use the `switchport vlan mapping` interface configuration command with the `dot1q-tunnel` keyword to map IEEE 802.1Q traffic with a specified outer and inner VLAN IDs to specified outer and inner VLAN IDs in the service-provider network. You can use the `drop` keyword to specify that traffic on a specified outer VLAN ID is dropped unless the specified inner and outer VLAN ID combination is explicitly translated.

Beginning in privileged EXEC mode, follow these steps on an ES port to configure the switch to drop or translate IEEE 802.1Q tagged traffic:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>interface interface-id Enter interface configuration mode and the ES interface connected to the service-provider network.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>switchport vlan mapping dot1q-tunnel outer-vlan-id {inner-vlan-id translated-vlan-id</td>
</tr>
<tr>
<td></td>
<td>• outer-vlan-id—Enter the outer VLAN ID of the original IEEE 802.1Q packet. The VLAN ID range is from 1 to 4094.</td>
</tr>
<tr>
<td></td>
<td>• inner-vlan-id translated-vlan-id—Enter the inner VLAN ID of the original IEEE 802.1Q packet and the translated VLAN ID for the service-provider network. The VLAN ID range is from 1 to 4094.</td>
</tr>
<tr>
<td></td>
<td>• drop—Specify that traffic with the specified outer VLAN ID is dropped unless the inner VLAN ID is matched in the existing VLAN mappings.</td>
</tr>
</tbody>
</table>
Configuring IEEE 802.1Q and Layer 2 Protocol Tunneling

Configuring IEEE 802.1ad

While QinQ is a Cisco-proprietary system to enable double-tagging to provide VLAN scalability in the provider network, IEEE 802.1ad uses standard protocols for VLAN scalability in provider networks. As with QinQ, data traffic entering from the customer interface is tagged with a service-provider tag. The customer frame crosses the provider network with two tags: the inner tag is the customer tag (C-tag), and the outer tag is the service-provider tag (S-tag). Control packets appear as data inside the provider network.

The Catalyst 3750 Metro switch supports these IEEE 802.1ad features:

- a switchport-based model
- all-to-one bundling
- service multiplexing (complex UNI)

In 802.1ad, a switchport is configured as either a customer user-network interface (C-UNI), a service-provider UNI (S-UNI), or a network-to-network interface (NNI). Only Layer 2 interfaces can be 802.1ad ports.

- C-UNI—can be either an access port or an 802.1Q trunk port. The port uses the customer bridge addresses. To configure a C-UNI port, enter the `ethernet dot1ad uni c-port` interface configuration command. New keywords added to the `switchport vlan mapping` interface configuration command allow all-to-one or selective bundling capability for customer VLANs when the interface is configured as an 802.1ad trunk C-UNI port.

  On a Catalyst 3750 Metro switch, you cannot configure an ES port as a C-UNI port.

- S-UNI—an access port that provides the same service to all customer VLANs entering the interface, marking all C-VLANs entering the port with the same S-VLAN. In this mode, the customer’s port is configured as a trunk port, and traffic entering the S-UNI is tagged. On S-UNIs, CDP and LLDP are disabled, and STP BPDU filtering and Port Fast are enabled. You can configure the port as an access port only; trunk configuration is not allowed.

  - CFM C-VLAN configuration is not allowed on an S-UNI.

  - You enter the `ethernet dot1ad uni s-port` interface configuration command to configure the port in dot1q-tunnel mode. You cannot configure an ES port as an S-UNI.

- NNI—entering the `ethernet dot1ad nni` interface command on a trunk port creates 802.1ad EtherType (0x88a8) and uses S-bridge addresses for CPU-generated Layer 2 protocol PDUs. Only trunk ports can be NNIs. CFM C-VLAN configuration is not allowed on an NNI.

  - Note: On a Catalyst 3750 Metro switch, you can configure 802.1ad NNIs only on ES ports. Non-ES ports can be configured as C-UNIs or S-UNIs.

See the command reference for more information on commands that support 802.1ad.

### 802.1ad Configuration Guidelines

- An S-UNI must be an access port.
- An NNI must be a trunk port.
- A C-UNI can be either an access port or a trunk port.
- On the Catalyst 3750 Metro switch, configure only ES ports as NNIs. Configure only non-ES ports as UNIs.
- 802.1ad is a port-based feature. There is no global command for enabling 802.1ad. By default, without 802.1ad, all switchports are traditional 802.1Q ports.
- When 802.1ad is enabled, the tunneling of customer data frames is done in software. If the incoming BPDU rate is high, there could be some impact on CPU utilization.
- The switches do not support 802.1ad on EVCs or 802.1ad Layer 3 termination.
The switches do not support split horizon on 802.1ad interfaces.

You cannot enable Layer 2 protocol tunneling on 802.1ad interfaces. The features are mutually exclusive.

Catalyst 3750 Metro switches support a mixed configuration model for 802.1ad that allows traditional QinQ tunnels and 802.1ad tunnels on a bridge at the same time. When configuring a switch in mixed configuration mode, be sure to separate the broadcast domains for traditional 802.1Q tunneling and 802.1ad tunneling. To ensure functionality, do not configure 802.1ad NNI trunk ports and 802.1Q egress trunks with overlapping sets of allowed VLANs.

By default, customer UDLD packets are tunneled on 802.1ad S-UNI ports and are processed (peered) on C-UNI ports. End-to-end UDLD is not supported on 802.1ad C-UNI ports.

When configuring the service provider network for 802.1ad, be sure to configure 802.1ad NNIs on all interconnecting trunk ports. This is required for end-to-end functionality for customer Layer 2 PDUs in the service provider network.

Configuring 802.1ad on EtherChannels

When configuring 802.1ad on port channels, configure the EtherChannel group first, and then configure 802.1ad port configuration on the bundled port (port channel). When configured on the EtherChannel port channel, the 802.1ad configuration is applied to all ports in the port channel.

You cannot add a port to an EtherChannel if the port already has 802.1ad enabled.

Follow this configuration sequence when both CE and PE devices are actively participating in PAgP or LACP EtherChannels.

Configuration Example for 802.1ad End-to-End PAgP EtherChannels between CE Devices

See Figure 15-5. For end-to-end PAgP EtherChannel tunneling between CE devices, you should extend the CE connections through the service provider network as a point-to-point service when the PE device has no EtherChannels in on mode. See the software configuration guide section “Configuring Layer 2 Tunneling for EtherChannels” in the “Configuring IEEE 802.1Q and Layer 2 Protocol Tunneling” chapter. The same procedure applies to 802.1ad tunnels.
Chapter 15 Configuring IEEE 802.1Q and Layer 2 Protocol Tunneling

Figure 15-5 802.1ad End-to-End PAgP EtherChannels

Configuration on Customer A1:

Switch #show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
Number of channel-groups in use:  2
Number of aggregators:             2

<table>
<thead>
<tr>
<th>Group</th>
<th>Port-channel</th>
<th>Protocol</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>23</td>
<td>Po23(SU)</td>
<td>PAgP (desirable)</td>
<td>Fa1/0/2(P) Fa1/0/3(P) Fa1/0/4(P)</td>
</tr>
</tbody>
</table>

Configuration on PE-1:

Switch (config)# interface GigabitEthernet0/2
Switch (config-if)# switchport access vlan 4002
Switch (config-if)# ethernet dot1ad uni s-port
Switch (config)# interface GigabitEthernet0/2
Switch (config-if)# switchport access vlan 4002
Switch (config-if)# switchport mode trunk

Switch (config)# interface GigabitEthernet0/3
Switch (config-if)# switchport access vlan 4001
Switch (config-if)# ethernet dot1ad uni s-port
Switch (config-if)# switchport trunk allowed vlan 4002
Switch (config-if)# switchport vlan mapping default dot1ad-bundle
Switch (config-if)# Ethernet dot1ad uni c-port

Switch (config)# interface GigabitEthernet0/4
Switch (config-if)# switchport access vlan 4003
Switch (config-if)# ethernet dot1ad uni s-port

Switch (config)# interface GigabitEthernet0/10
Switch (config-if)# switchport trunk allowed vlan 4001-4094
Switch (config-if)# switchport mode trunk
Switch (config-if)# media-type sfp
Switch (config-if)# ethernet dot1ad nni

Configuration on PE-3

Switch (config)# interface GigabitEthernet1/1/1
Switch (config-if)# switchport trunk allowed vlan 4001-4094
Switch (config-if)# switchport mode trunk
Switch (config-if)# switchport trunk dot1q ethertype 88A8
Switch (config-if)# udl port aggressive
Switch (config-if)# ethernet dot1ad nni

Switch (config)# interface GigabitEthernet1/1/2
Switch (config-if)# switchport trunk allowed vlan 4001-4094
Switch (config-if)# switchport mode trunk
Switch (config-if)# switchport trunk dot1q ethertype 88A8
Switch (config-if)# udl port aggressive
Switch (config-if)# ethernet dot1ad nni

Configuration on PE-2

Switch (config)# interface GigabitEthernet0/9
Switch (config-if)# switchport access vlan 4002
Switch (config-if)# ethernet dot1ad uni s-port

Switch (config)# interface GigabitEthernet0/10
Switch (config-if)# switchport access vlan 4001
Switch (config-if)# ethernet dot1ad uni s-port

Switch (config)# interface GigabitEthernet0/11
Switch (config-if)# switchport access vlan 4003
Switch (config-if)# ethernet dot1ad uni s-port

Switch (config)# interface GigabitEthernet0/13
Switch (config-if)# switchport trunk allowed vlan 4001-4094
Switch (config-if)# switchport mode trunk
Switch (config-if)# ethernet dot1ad nni

Configuration on Customer A3

Switch (config)# interface Port-channel23
Switch (config-if)# switchport trunk encapsulation dot1q
Switch (config-if)# switchport mode trunk

Switch (config)# interface FastEthernet1/0/21
Switch (config-if)# switchport trunk encapsulation dot1q
Switch (config-if)# switchport mode trunk
Switch (config-if)# channel-protocol pagp
Switch (config-if)# channel-group 23 mode desirable

Switch (config)# interface FastEthernet1/0/2
Switch (config-if)# switchport trunk encapsulation dot1q
Switch (config-if)# switchport mode trunk
Switch (config-if)# channel-protocol pagp
Switch (config-if)# channel-group 23 mode desirable

Switch (config)# interface FastEthernet1/0/23
Switch (config-if)# switchport trunk encapsulation dot1q
Switch (config-if)# switchport mode trunk
Switch (config-if)# channel-protocol pagp
Switch (config-if)# channel-group 23 mode desirable

Configuration with 802.1ad C-UNI port on PE-2 and PE-3

Switch (config)# interface GigabitEthernet0/2
Switch (config-if)# switchport access vlan 4002
Switch (config-if)# switchport mode trunk
Switch (config-if)# switchport trunk allowed vlan 4002
Switch (config-if)# switchport vlan mapping default dot1ad-bundle 4002
Switch (config-if)# Ethernet dot1ad uni c-port

Switch (config)# interface GigabitEthernet0/3
Switch (config-if)# switchport access vlan 4001
Switch (config-if)# switchport mode trunk
Switch (config-if)# switchport trunk allowed vlan 4001
Switch (config-if)# switchport vlan mapping default dot1ad-bundle 4001
Switch (config-if)# Ethernet dot1ad uni c-port

Switch (config)# interface GigabitEthernet0/4
Switch (config-if)# switchport access vlan 4003
Switch (config-if)# switchport mode trunk
Switch (config-if)# switchport trunk allowed vlan 4003
Switch (config-if)# switchport vlan mapping default dot1ad-bundle 4003
Switch (config-if)# Ethernet dot1ad uni c-port

The configuration on other switches remains the same in the 802.1ad C-UNI scenario.
Understanding Layer 2 Protocol Tunneling

Customers at different sites connected across a service-provider network need to run various Layer 2 protocols to scale their topology to include all remote sites, as well as the local sites. STP must run properly, and every VLAN should build a proper spanning tree that includes the local site and all remote sites across the service-provider infrastructure. Cisco Discovery Protocol (CDP) must discover neighboring Cisco devices from local and remote sites. VLAN Trunking Protocol (VTP) must provide consistent VLAN configuration throughout all sites in the customer network.

When protocol tunneling is enabled, edge switches on the inbound side of the service-provider infrastructure encapsulate Layer 2 protocol packets with a special MAC address and send them across the service-provider network. Core switches in the network do not process these packets but forward them as normal packets. Layer 2 protocol data units (PDUs) for CDP, STP, or VTP cross the service-provider infrastructure and are delivered to customer switches on the outbound side of the service-provider network. Identical packets are received by all customer ports on the same VLANs with these results:

- Users on each of a customer’s sites are able to properly run STP, and every VLAN can build a correct spanning tree based on parameters from all sites and not just from the local site.
- CDP discovers and shows information about the other Cisco devices connected through the service-provider network.
- VTP provides consistent VLAN configuration throughout the customer network, propagating through the service provider to all switches.

To provide interoperability with third-party vendors, you can use the Layer 2 protocol-tunnel bypass feature. Bypass mode transparently forwards control PDUs to vendor switches that have different ways of controlling protocol tunneling. You implement bypass mode by enabling Layer 2 protocol tunneling on the egress trunk port. When Layer 2 protocol tunneling is enabled on the trunk port, the encapsulated tunnel MAC address is removed and the protocol packets have their normal MAC address.

Layer 2 protocol tunneling can be used independently or can enhance IEEE 802.1Q tunneling. If protocol tunneling is not enabled on IEEE 802.1Q tunneling ports, remote switches at the receiving end of the service-provider network do not receive the PDUs and cannot properly run STP, CDP, and VTP. When protocol tunneling is enabled, Layer 2 protocols within each customer’s network are totally separate from those running within the service-provider network. Customer switches on different sites that send traffic through the service-provider network with IEEE 802.1Q tunneling achieve complete knowledge of the customer’s VLAN. If IEEE 802.1Q tunneling is not used, you can still enable Layer 2 protocol tunneling by connecting to the customer switch through access ports or trunk ports and enabling tunneling on the service-provider access or trunk port.

For example, in Figure 15-6, Customer X has four switches in the same VLAN that are connected through the service-provider network. If the network does not tunnel PDUs, switches on the far ends of the network cannot properly run STP, CDP, and VTP. For example, STP for a VLAN on a switch in Customer X, Site 1 will build a spanning tree on the switches at that site without considering convergence parameters based on Customer X’s switch in Site 2. This could result in the topology shown in Figure 15-7.
In a service-provider network, you can use Layer 2 protocol tunneling to enhance the creation of EtherChannels by emulating a point-to-point network topology. When you enable protocol tunneling (PAgP or LACP) on the service-provider switch, remote customer switches receive the PDUs and can negotiate the automatic creation of EtherChannels.
For example, in Figure 15-8, Customer A has two switches in the same VLAN that are connected through the SP network. When the network tunnels PDUs, switches on the far ends of the network can negotiate the automatic creation of EtherChannels without needing dedicated lines. See the “Configuring Layer 2 Tunneling for EtherChannels” section on page 15-23 for instructions on configuring Layer 2 protocol tunneling for EtherChannels.

Figure 15-8 Layer 2 Protocol Tunneling for EtherChannels

Configuring Layer 2 Protocol Tunneling

You enable Layer 2 protocol tunneling (by protocol) on the ports that are connected to the customer in the edge switches of the service-provider network. Edge-switch tunnel ports are connected to customer IEEE 802.1Q trunk ports; edge-switch access ports are connected to customer access ports. The edge switches connected to the customer switch perform the tunneling process.

You can enable Layer 2 protocol tunneling on ports that are configured as access ports, tunnel ports, or trunk ports. You cannot enable Layer 2 protocol tunneling on ports configured in either switchport mode dynamic auto (the default mode), or switchport mode dynamic desirable. The switch supports Layer 2 protocol tunneling for CDP, STP, and VTP. For emulated point-to-point network topologies, it also supports PAgP, LACP, and UDLD protocols. The switch does not support Layer 2 protocol tunneling for LLDP.

Caution

PAgP, LACP, and UDLD protocol tunneling is only intended to emulate a point-to-point topology. An erroneous configuration that sends tunneled packets to many ports could lead to a network failure.

When the Layer 2 PDUs that entered the inbound edge switch through a Layer 2 protocol-enabled port exit the switch through the trunk port into the service-provider network, the switch overwrites the customer PDU-destination MAC address with a well-known Cisco proprietary multicast address (01-00-0c-cd-cd-d0). If IEEE 802.1Q tunneling is enabled, packets are also double-tagged; the outer tag is the customer metro tag and the inner tag is the customer VLAN tag. The core switches ignore the inner tags and forward the packet to all trunk ports in the same metro VLAN. The edge switches on the outbound side restore the proper Layer 2 protocol and MAC address information and forward the packets to all tunnel ports, access ports, and Layer 2 protocol-enabled trunk ports in the same metro VLAN. Therefore, the Layer 2 PDUs are kept intact and delivered across the service-provider infrastructure to the other side of the customer network.
Configuring Layer 2 Protocol Tunneling

See Figure 15-6, with Customer X and Customer Y in access VLANs 30 and 40, respectively. Asymmetric links connect the customers in Site 1 to edge switches in the service-provider network. The Layer 2 PDUs (for example, BPDUs) coming into Switch B from Customer Y in Site 1 are forwarded to the infrastructure as double-tagged packets with the well-known MAC address as the destination MAC address. These double-tagged packets have the outer VLAN tag of 40 as well as an inner VLAN tag (for example, VLAN 100). When the double-tagged packets reach Switch D, the outer VLAN tag 40 is removed, the well-known MAC address is replaced with the respective Layer 2 protocol MAC address, and the packet is sent to Customer Y on Site 2 as a single-tagged frame in VLAN 100.

You can also enable Layer 2 protocol tunneling on access or trunk ports on the edge switch connected to access or trunk ports on the customer switch. In this case, the encapsulation and de-encapsulation behavior is the same as described in the previous paragraph, except that the packets are not double-tagged in the service-provider network. The single tag is the customer-specific access VLAN tag.

This section contains this information about configuring Layer 2 protocol tunneling:

- Default Layer 2 Protocol Tunneling Configuration, page 15-20
- Configuring Layer 2 Tunneling, page 15-22
- Configuring Layer 2 Tunneling for EtherChannels, page 15-23

Default Layer 2 Protocol Tunneling Configuration

Table 15-1 shows the default Layer 2 protocol tunneling configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 2 protocol tunneling</td>
<td>Disabled for CDP, STP, and VTP.</td>
</tr>
<tr>
<td>Shutdown threshold</td>
<td>No threshold for packets-per-second of Layer 2 PDUs per port for the port to shut down.</td>
</tr>
<tr>
<td>Drop threshold</td>
<td>No threshold for packets-per-second of Layer 2 PDUs per port for the port to drop the PDUs.</td>
</tr>
<tr>
<td>Class of service (CoS) value</td>
<td>If a CoS value is configured on the interface, that value is used to set the BPDU CoS value for Layer 2 protocol tunneling. If no CoS value is configured at the interface level, the default value for CoS marking of L2 protocol tunneling BPDU is 5. This does not apply to data traffic.</td>
</tr>
</tbody>
</table>

Layer 2 Protocol Tunneling Configuration Guidelines

These are some configuration guidelines and operating characteristics of Layer 2 protocol tunneling:

- The switch supports tunneling of CDP, STP, including multiple STP (MSTP), and VTP. Protocol tunneling is disabled by default but can be enabled for the individual protocols on IEEE 802.1Q tunnel ports, access ports, or trunk ports.
- The switch supports PAgP, LACP, and UDLD tunneling for emulated point-to-point network topologies. Protocol tunneling is disabled by default but can be enabled for the individual protocols on IEEE 802.1Q tunnel ports, access ports, or trunk ports.
The switch does not support Layer 2 protocol tunneling on ports with switchport mode **dynamic auto** or **dynamic desirable**.

If you enable PAgP or LACP tunneling, we recommend that you also enable UDLD on the interface for faster link-failure detection.

Loopback detection is not supported on Layer 2 protocol tunneling of PAgP, LACP, or UDLD packets.

Dynamic Trunking Protocol (DTP) is not compatible with Layer 2 protocol tunneling because you must manually configure asymmetric links with tunnel ports and trunk ports.

The edge switches on the outbound side restore the proper Layer 2 protocol and MAC address information and forward the packets to all tunnel ports, access ports and Layer 2 protocol-enabled trunk ports in the same metro VLAN.

For interoperability with third-party vendor switches, the switch supports a Layer 2 protocol-tunnel bypass feature. Bypass mode transparently forwards control PDUs to vendor switches that have different ways of controlling protocol tunneling. When Layer 2 protocol tunneling is enabled on ingress ports on a switch, egress trunk ports forward the tunneled packets with a special encapsulation. If you also enable Layer 2 protocol tunneling on the egress trunk port, this behavior is bypassed and the switch forwards control PDUs without any processing or modification.

EtherChannel port groups are compatible with tunnel ports as long as the IEEE 802.1Q configuration is consistent within an EtherChannel port group.

If an encapsulated PDU (with the proprietary destination MAC address) is received from a tunnel port or access or trunk port with Layer 2 tunneling enabled, the port is shut down to prevent loops. The port also shuts down when a configured shutdown threshold for the protocol is reached. You can manually re-enable the port (by entering a `shutdown` and `no shutdown` command sequence) or if errdisable recovery is enabled, the operation is retried after a specified time interval.

Only decapsulated PDUs are forwarded to the customer network. The spanning-tree instance running on the service-provider network does not forward BPDUs to tunnel ports. No CDP packets are forwarded from tunnel ports.

When protocol tunneling is enabled on an interface, you can set a per-protocol, per-port, shutdown threshold for the PDUs generated by the customer network. If the limit is exceeded, the port shuts down. You can also rate-limit BPDUs by using QoS ACLs and policy maps on a tunnel port.

When protocol tunneling is enabled on an interface, you can set a per-protocol, per-port, drop threshold for the PDUs generated by the customer network. If the limit is exceeded, the port drops PDUs until the rate at which the port receives them is below the drop threshold.

Because tunneled PDUs (especially STP BPDUs) must be delivered to all remote sites for the customer virtual network to operate properly, you can give PDUs higher priority within the service-provider network than data packets received from the same tunnel port. By default, the PDUs use the same CoS value as data packets.
## Configuring Layer 2 Tunneling

Beginning in privileged EXEC mode, follow these steps to configure a port for Layer 2 protocol tunneling:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td></td>
<td>Enter the interface configuration mode and the interface to be configured as a tunnel port. This should be the edge port in the service-provider network that connects to the customer switch. Valid interfaces include physical interfaces and port-channel logical interfaces (port channels 1 to 12).</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>switchport mode access or switchport mode dot1q-tunnel or switchport mode trunk</td>
</tr>
<tr>
<td></td>
<td>Configure the interface as an access port, an IEEE 802.1Q tunnel port or a trunk port.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>l2protocol-tunnel [cdp</td>
</tr>
<tr>
<td></td>
<td>Enable protocol tunneling for the desired protocol. If no keyword is entered, tunneling is enabled for all three Layer 2 protocols.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>l2protocol-tunnel shutdown-threshold [cdp</td>
</tr>
<tr>
<td></td>
<td>(Optional) Configure the threshold in packets per second to be received for encapsulation before the interface shuts down. The port is disabled if the configured threshold is exceeded. If no protocol option is specified, the threshold is applied to each of the tunneled Layer 2 protocol types. The range is 1 to 4096. The default is to have no threshold configured.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>If you also set a drop threshold on this interface, the shutdown-threshold value must be greater than or equal to the drop-threshold value.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>l2protocol-tunnel drop-threshold [cdp</td>
</tr>
<tr>
<td></td>
<td>(Optional) Configure the threshold in packets per second to be received for encapsulation before the interface drops packets. The port drops packets if the configured threshold is exceeded. If no protocol option is specified, the threshold is applied to each of the tunneled Layer 2 protocol types. The range is 1 to 4096. The default is to have no threshold configured.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>If you also set a shutdown threshold on this interface, the drop-threshold value must be less than or equal to the shutdown-threshold value.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>exit</td>
</tr>
<tr>
<td></td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>errdisable recovery cause l2ptguard</td>
</tr>
<tr>
<td></td>
<td>(Optional) Configure the recovery mechanism from a Layer 2 maximum rate error so that the interface can be brought out of the disabled state and allowed to try again. You can also set the time interval. Errdisable recovery is disabled by default; when enabled, the default time interval is 300 seconds.</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>l2protocol-tunnel cos value</td>
</tr>
<tr>
<td></td>
<td>(Optional) Configure the CoS value for all tunneled Layer 2 PDUs. The range is 0 to 7; the default is the default CoS value for the interface. If none is configured, the default is 5.</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>end</td>
</tr>
<tr>
<td></td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
Chapter 15      Configuring IEEE 802.1Q and Layer 2 Protocol Tunneling

Configuring Layer 2 Protocol Tunneling

Use the `no l2protocol-tunnel [cdp | stp | vtp]` interface configuration command to disable protocol tunneling for one of the Layer 2 protocols or for all three of them. Use the `no l2protocol-tunnel shutdown-threshold [cdp | stp | vtp]` and the `no l2protocol-tunnel drop-threshold [cdp | stp | vtp]` commands to return the shutdown and drop thresholds to the default settings.

This example shows how to configure Layer 2 protocol tunneling for CDP, STP, and VTP and to verify the configuration.

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# l2protocol-tunnel cdp
Switch(config-if)# l2protocol-tunnel stp
Switch(config-if)# l2protocol-tunnel vtp
Switch(config-if)# l2protocol-tunnel shutdown-threshold 1500
Switch(config-if)# l2protocol-tunnel drop-threshold 1000
Switch(config-if)# exit
Switch(config)# l2protocol-tunnel cos 7
Switch(config)# end
Switch# show l2protocol
COS for Encapsulated Packets: 7

Port   Protocol  Shutdown Threshold  Drop Threshold  Encapsulation Counter  Decapsulation Counter  Drop Counter
------- -------- --------- --------- ------------- ------------- --------------
Gi1/0/2  cdp      1500      1000             0             0             0
         stp      1500      1000             0             0             0
         vtp      1500      1000             0             0             0
```

Configuring Layer 2 Tunneling for EtherChannels

To configure Layer 2 point-to-point tunneling to facilitate the automatic creation of EtherChannels, you need to configure both the service-provider edge switch and the customer switch.

Configuring the Service-Provider Edge Switch

Beginning in privileged EXEC mode, follow these steps to configure a service-provider edge switch for Layer 2 protocol tunneling for EtherChannels:

```
Step 1 configure terminal
Purpose
Enter global configuration mode.

Step 2 interface interface-id
Purpose
Enter interface configuration mode, and enter the interface to be configured as a tunnel port. This should be the edge port in the service-provider network that connects to the customer switch. Valid interfaces are physical interfaces.

Step 3 switchport mode dot1q-tunnel
Purpose
Configure the interface as an IEEE 802.1Q tunnel port.
```
## Step 4

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>l2protocol-tunnel point-to-point [pagp</td>
<td>lacp</td>
</tr>
</tbody>
</table>

**Caution** To avoid a network failure, make sure that the network is a point-to-point topology before you enable tunneling for PAgP, LACP, or UDLD packets.

## Step 5

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>l2protocol-tunnel shutdown-threshold [point-to-point [pagp</td>
<td>lacp</td>
</tr>
</tbody>
</table>

**Note** If you also set a drop threshold on this interface, the shutdown-threshold value must be greater than or equal to the drop-threshold value.

## Step 6

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>l2protocol-tunnel drop-threshold [point-to-point [pagp</td>
<td>lacp</td>
</tr>
</tbody>
</table>

**Note** If you also set a shutdown threshold on this interface, the drop-threshold value must be less than or equal to the shutdown-threshold value.

## Step 7

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>no cdp enable</td>
<td>Disable CDP on the interface.</td>
</tr>
</tbody>
</table>

## Step 8

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>spanning-tree bpdufilter enable</td>
<td>Enable BPDU filtering on the interface.</td>
</tr>
</tbody>
</table>

## Step 9

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>exit</td>
<td>Return to global configuration mode.</td>
</tr>
</tbody>
</table>

## Step 10

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>errdisable recovery cause l2ptguard</td>
<td>(Optional) Configure the recovery mechanism from a Layer 2 maximum-rate error so that the interface is re-enabled and can try again. Errdisable recovery is disabled by default; when enabled, the default time interval is 300 seconds.</td>
</tr>
</tbody>
</table>

## Step 11

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>l2protocol-tunnel cos value</td>
<td>(Optional) Configure the CoS value for all tunneled Layer 2 PDUs. The range is 0 to 7; the default is the default CoS value for the interface. If none is configured, the default is 5.</td>
</tr>
</tbody>
</table>

## Step 12

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

## Step 13

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show l2protocol</td>
<td>Display the Layer 2 tunnel ports on the switch, including the protocols configured, the thresholds, and the counters.</td>
</tr>
</tbody>
</table>

## Step 14

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Use the no l2protocol-tunnel [point-to-point [pagp | lacp | udld]] interface configuration command to disable point-to-point protocol tunneling for one of the Layer 2 protocols or for all three. Use the no l2protocol-tunnel shutdown-threshold [point-to-point [pagp | lacp | udld]] and the no l2protocol-tunnel drop-threshold [[point-to-point [pagp | lacp | udld]] commands to return the shutdown and drop thresholds to the default settings.
Chapter 15      Configuring IEEE 802.1Q and Layer 2 Protocol Tunneling

Configuring the Customer Switch

After configuring the service-provider edge switch, begin in privileged EXEC mode and follow these steps to configure a customer switch for Layer 2 protocol tunneling for EtherChannels:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>switchport trunk encapsulation dot1q</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>switchport mode trunk</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>udld enable</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>channel-group channel-group-number mode desirable</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>exit</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>interface port-channel port-channel number</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>shutdown</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>no shutdown</td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td>show l2protocol</td>
</tr>
<tr>
<td><strong>Step 13</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

Use the **no switchport mode trunk**, **no udld enable**, and the **no channel group channel-group-number mode desirable** interface configuration commands to return the interface to the default settings.

For EtherChannels, you need to configure both the service-provider edge switches and the customer switches for Layer 2 protocol tunneling.

This example shows how to configure the service provider edge Switch A and edge Switch B in the example in Figure 15-8 on page 15-19. VLANs 17, 18, 19, and 20 are the access VLANs, Fast Ethernet ports 1 and 2 are point-to-point tunnel ports with PAgP and UDLD enabled, the drop threshold is 1000, and Fast Ethernet port 3 is a trunk port.

Service-provider edge Switch A configuration:

```
Switch(config)# interface fastethernet1/0/1
Switch(config-if)# switchport access vlan 17
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# l2protocol-tunnel point-to-point pagp
Switch(config-if)# l2protocol-tunnel point-to-point udld
Switch(config-if)# l2protocol-tunnel drop-threshold point-to-point pagp 1000
Switch(config-if)# exit
Switch(config)# interface fastethernet1/0/2
```
Configuring Layer 2 Protocol Tunneling

Switch(config-if)# switchport access vlan 18
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# l2protocol-tunnel point-to-point pagp
Switch(config-if)# l2protocol-tunnel point-to-point udld
Switch(config-if)# l2protocol-tunnel drop-threshold point-to-point pagp 1000
Switch(config-if)# exit
Switch(config)# interface fastethernet1/0/3
Switch(config-if)# switchport trunk encapsulation isl
Switch(config-if)# switchport mode trunk

Service-provider edge Switch B configuration:

Switch(config)# interface fastethernet1/0/1
Switch(config-if)# switchport access vlan 19
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# l2protocol-tunnel point-to-point pagp
Switch(config-if)# l2protocol-tunnel point-to-point udld
Switch(config-if)# l2protocol-tunnel drop-threshold point-to-point pagp 1000
Switch(config-if)# exit
Switch(config)# interface fastethernet1/0/2
Switch(config-if)# switchport access vlan 20
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# l2protocol-tunnel point-to-point pagp
Switch(config-if)# l2protocol-tunnel point-to-point udld
Switch(config-if)# l2protocol-tunnel drop-threshold point-to-point pagp 1000
Switch(config-if)# exit
Switch(config)# interface fastethernet1/0/3
Switch(config-if)# switchport trunk encapsulation isl
Switch(config-if)# switchport mode trunk

This example shows how to configure the customer switch at Site 1. Fast Ethernet ports 1, 2, 3, and 4 are set for IEEE 802.1Q trunking, UDLD is enabled, EtherChannel group 1 is enabled, and the port channel is shut down and then enabled to activate the EtherChannel configuration.

Switch(config)# interface fastethernet1/0/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# udld enable
Switch(config-if)# channel-group 1 mode desirable
Switch(config-if)# exit
Switch(config)# interface fastethernet1/0/2
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# udld enable
Switch(config-if)# channel-group 1 mode desirable
Switch(config-if)# exit
Switch(config)# interface fastethernet1/0/3
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# udld enable
Switch(config-if)# channel-group 1 mode desirable
Switch(config-if)# exit
Switch(config)# interface fastethernet1/0/4
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# udld enable
Switch(config-if)# channel-group 1 mode desirable
Switch(config-if)# exit
Switch(config)# interface port-channel 1
Switch(config-if)# shutdown
Switch(config-if)# no shutdown
Switch(config-if)# exit
### Monitoring and Maintaining Tunneling and Mapping Status

Table 15-2 shows the privileged EXEC commands for monitoring and maintaining IEEE 802.1Q and Layer 2 protocol tunneling and VLAN mapping.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear l2protocol-tunnel counters</td>
<td>Clear the protocol counters on Layer 2 protocol tunneling ports.</td>
</tr>
<tr>
<td>show dot1q-tunnel</td>
<td>Display IEEE 802.1Q tunnel ports on the switch.</td>
</tr>
<tr>
<td>show dot1q-tunnel interface interface-id</td>
<td>Verify if a specific interface is a tunnel port.</td>
</tr>
<tr>
<td>show l2protocol-tunnel</td>
<td>Display information about Layer 2 protocol tunneling ports.</td>
</tr>
<tr>
<td>show errdisable recovery</td>
<td>Verify if the recovery timer from a Layer 2 protocol-tunnel error disable state is enabled.</td>
</tr>
<tr>
<td>show interface interface-id vlan mapping</td>
<td>Display VLAN mapping information for the specified interface. The interface can be an ES port or a VLAN.</td>
</tr>
<tr>
<td>show l2protocol-tunnel interface interface-id</td>
<td>Display information about a specific Layer 2 protocol tunneling port.</td>
</tr>
<tr>
<td>show l2protocol-tunnel summary</td>
<td>Display only Layer 2 protocol summary information.</td>
</tr>
<tr>
<td>show vlan dot1q native</td>
<td>Display the status of native VLAN tagging on the switch.</td>
</tr>
<tr>
<td>show vlan mapping</td>
<td>Display VLAN mapping information (contents of the VLAN mapping table) for the ES ports.</td>
</tr>
</tbody>
</table>

For detailed information about these displays, see the command reference for this release.
Monitoring and Maintaining Tunneling and Mapping Status
Configuring STP

This chapter describes how to configure the Spanning Tree Protocol (STP) on port-based VLANs on the Catalyst 3750 Metro switch. The switch uses the per-VLAN spanning-tree plus (PVST+) protocol based on the IEEE 802.1D standard and Cisco proprietary extensions, or it can use the rapid per-VLAN spanning-tree plus (rapid-PVST+) protocol based on the IEEE 802.1w standard.

For information about the Multiple Spanning Tree Protocol (MSTP) and how to map multiple VLANs to the same spanning-tree instance, see Chapter 17, “Configuring MSTP.” For information about other spanning-tree features such as Port Fast, UplinkFast, root guard, and so forth, see Chapter 18, “Configuring Optional Spanning-Tree Features.”

For complete syntax and usage information for the commands used in this chapter, see the command reference for this release.

This chapter consists of these sections:

- Understanding Spanning-Tree Features, page 16-1
- Configuring Spanning-Tree Features, page 16-11
- Displaying the Spanning-Tree Status, page 16-22

Understanding Spanning-Tree Features

These sections describe how basic spanning-tree features work:

- STP Overview, page 16-2
- Spanning-Tree Topology and BPDUs, page 16-3
- Bridge ID, Switch Priority, and Extended System ID, page 16-4
- Spanning-Tree Interface States, page 16-4
- How a Switch or Port Becomes the Root Switch or Root Port, page 16-7
- Spanning Tree and Redundant Connectivity, page 16-8
- Spanning-Tree Address Management, page 16-8
- Accelerated Aging to Retain Connectivity, page 16-8
- Spanning-Tree Modes and Protocols, page 16-9
- Supported Spanning-Tree Instances, page 16-9
STP Overview

STP is a Layer 2 link management protocol that provides path redundancy while preventing loops in the network. For a Layer 2 Ethernet network to function properly, only one active path can exist between any two stations. Multiple active paths among end stations cause loops in the network. If a loop exists in the network, end stations might receive duplicate messages. Switches might also learn end-station MAC addresses on multiple Layer 2 interfaces. These conditions result in an unstable network. Spanning-tree operation is transparent to end stations, which cannot detect whether they are connected to a single LAN segment or a switched LAN of multiple segments.

The STP uses a spanning-tree algorithm to select one switch of a redundantly connected network as the root of the spanning tree. The algorithm calculates the best loop-free path through a switched Layer 2 network by assigning a role to each port based on the role of the port in the active topology:

- **Root**—A forwarding port elected for the spanning-tree topology
- **Designated**—A forwarding port elected for every switched LAN segment
- **Alternate**—A blocked port providing an alternate path to the root bridge in the spanning tree
- **Backup**—A blocked port in a loopback configuration

The switch that has all of its ports as the designated role or as the backup role is the root switch. The switch that has at least one of its ports in the designated role is called the designated switch.

Spanning tree forces redundant data paths into a standby (blocked) state. If a network segment in the spanning tree fails and a redundant path exists, the spanning-tree algorithm recalculates the spanning-tree topology and activates the standby path. Switches send and receive spanning-tree frames, called bridge protocol data units (BPDUs), at regular intervals. The switches do not forward these frames but use them to construct a loop-free path. BPDUs contain information about the sending switch and its ports, including switch and MAC addresses, switch priority, port priority, and path cost. Spanning tree uses this information to elect the root switch and root port for the switched network and the root port and designated port for each switched segment.

When two ports on a switch are part of a loop, the spanning-tree port priority and path cost settings control which port is put in the forwarding state and which is put in the blocking state. The spanning-tree port priority value represents the location of a port in the network topology and how well it is located to pass traffic. The path cost value represents the media speed.

---

**Note**

In Cisco IOS Release 12.2(25)EY and later releases, the switch sends keepalive messages (to ensure the connection is up) only on interfaces that do not have small form-factor pluggable (SFP) modules.
Spanning-Tree Topology and BPDUs

The stable, active spanning-tree topology of a switched network is controlled by these elements:

- The unique bridge ID (switch priority and MAC address) associated with each VLAN on each switch.
- The spanning-tree path cost to the root switch.
- The port identifier (port priority and MAC address) associated with each Layer 2 interface.

When the switches in a network are powered up, each functions as the root switch. Each switch sends a configuration BPDU through all of its ports. The BPDUs communicate and compute the spanning-tree topology. Each configuration BPDU contains this information:

- The unique bridge ID of the switch that the sending switch identifies as the root switch
- The spanning-tree path cost to the root
- The bridge ID of the sending switch
- Message age
- The identifier of the sending interface
- Values for the hello, forward delay, and max-age protocol timers

When a switch receives a configuration BPDU that contains superior information (lower bridge ID, lower path cost, and so forth), it stores the information for that port. If this BPDU is received on the root port of the switch, the switch also forwards it with an updated message to all attached LANs for which it is the designated switch.

If a switch receives a configuration BPDU that contains inferior information to that currently stored for that port, it discards the BPDU. If the switch is a designated switch for the LAN from which the inferior BPDU was received, it sends that LAN a BPDU containing the up-to-date information stored for that port. In this way, inferior information is discarded, and superior information is propagated on the network.

A BPDU exchange results in these actions:

- One switch in the network is elected as the root switch (the logical center of the spanning-tree topology in a switched network).
  
  For each VLAN, the switch with the highest switch priority (the lowest numerical priority value) is elected as the root switch. If all switches are configured with the default priority (32768), the switch with the lowest MAC address in the VLAN becomes the root switch. The switch priority value occupies the most significant bits of the bridge ID, as shown in Table 16-1 on page 16-4.

- A root port is selected for each switch (except the root switch). This port provides the best path (lowest cost) when the switch forwards packets to the root switch.

- The shortest distance to the root switch is calculated for each switch based on the path cost.

- A designated switch for each LAN segment is selected. The designated switch incurs the lowest path cost when forwarding packets from that LAN to the root switch. The port through which the designated switch is attached to the LAN is called the designated port.

All paths that are not needed to reach the root switch from anywhere in the switched network are placed in the spanning-tree blocking mode.
Bridge ID, Switch Priority, and Extended System ID

The IEEE 802.1D standard requires that each switch has a unique bridge identifier (bridge ID), which controls the selection of the root switch. Because each VLAN is considered as a different logical bridge with PVST+ and rapid PVST+, the same switch must have as many different bridge IDs as VLANs configured on it. Each VLAN on the switch has a unique 8-byte bridge ID. The two most-significant bytes are used for the switch priority, and the remaining six bytes are derived from the switch MAC address.

The switch supports the 802.1t spanning-tree extensions, and some of the bits previously used for the switch priority are now used as the VLAN identifier. The result is that fewer MAC addresses are reserved for the switch, and a larger range of VLAN IDs can be supported, all while maintaining the uniqueness of the bridge ID. As shown in Table 16-1, the two bytes previously used for the switch priority are reallocated into a 4-bit priority value and a 12-bit extended system ID value equal to the VLAN ID.

Spanning tree uses the extended system ID, the switch priority, and the allocated spanning-tree MAC address to make the bridge ID unique for each VLAN.

Support for the extended system ID affects how you manually configure the root switch, the secondary root switch, and the switch priority of a VLAN. For example, when you change the switch priority value, you change the probability that the switch will be elected as the root switch. Configuring a higher value decreases the probability; a lower value increases the probability. For more information, see the “Configuring the Root Switch” section on page 16-14, the “Configuring a Secondary Root Switch” section on page 16-16, and the “Configuring the Switch Priority of a VLAN” section on page 16-19.

Spanning-Tree Interface States

Propagation delays can occur when protocol information passes through a switched LAN. As a result, topology changes can take place at different times and at different places in a switched network. When an interface transitions directly from nonparticipation in the spanning-tree topology to the forwarding state, it can create temporary data loops. Interfaces must wait for new topology information to propagate through the switched LAN before starting to forward frames. They must allow the frame lifetime to expire for forwarded frames that have used the old topology.

Each Layer 2 interface on a switch using spanning tree exists in one of these states:

- **Blocking**—The interface does not participate in frame forwarding.
- **Listening**—The first transitional state after the blocking state when the spanning tree determines that the interface should participate in frame forwarding.
- **Learning**—The interface prepares to participate in frame forwarding.
- **Forwarding**—The interface forwards frames.
- **Disabled**—The interface is not participating in spanning tree because of a shutdown port, no link on the port, or no spanning-tree instance running on the port.

<table>
<thead>
<tr>
<th>Switch Priority Value</th>
<th>Extended System ID (Set Equal to the VLAN ID)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bit 16</td>
<td>Bit 15</td>
</tr>
<tr>
<td>32768</td>
<td>16384</td>
</tr>
</tbody>
</table>
An interface moves through these states:

- From initialization to blocking
- From blocking to listening or to disabled
- From listening to learning or to disabled
- From learning to forwarding or to disabled
- From forwarding to disabled

*Figure 16-1* illustrates how an interface moves through the states.

*Figure 16-1  Spanning-Tree Interface States*

When you power up the switch, spanning tree is enabled by default, and every interface in the switch, VLAN, or network goes through the blocking state and the transitory states of listening and learning. Spanning tree stabilizes each interface at the forwarding or blocking state.

When the spanning-tree algorithm places a Layer 2 interface in the forwarding state, this process occurs:

1. The interface is in the listening state while spanning tree waits for protocol information to transition the interface to the blocking state.
2. While spanning tree waits the forward-delay timer to expire, it moves the interface to the learning state and resets the forward-delay timer.
3. In the learning state, the interface continues to block frame forwarding as the switch learns end-station location information for the forwarding database.
4. When the forward-delay timer expires, spanning tree moves the interface to the forwarding state, where both learning and frame forwarding are enabled.

**Blocking State**

A Layer 2 interface in the blocking state does not participate in frame forwarding. After initialization, a BPDU is sent to each switch interface. A switch initially functions as the root until it exchanges BPDUs with other switches. This exchange establishes which switch in the network is the root or root switch. If
there is only one switch in the network, no exchange occurs, the forward-delay timer expires, and the interface moves to the listening state. An interface always enters the blocking state after switch initialization.

An interface in the blocking state performs these functions:
- Discards frames received on the interface
- Discards frames switched from another interface for forwarding
- Does not learn addresses
- Receives BPDUs

Listening State

The listening state is the first state a Layer 2 interface enters after the blocking state. The interface enters this state when the spanning tree determines that the interface should participate in frame forwarding.

An interface in the listening state performs these functions:
- Discards frames received on the interface
- Discards frames switched from another interface for forwarding
- Does not learn addresses
- Receives BPDUs

Learning State

A Layer 2 interface in the learning state prepares to participate in frame forwarding. The interface enters the learning state from the listening state.

An interface in the learning state performs these functions:
- Discards frames received on the interface
- Discards frames switched from another interface for forwarding
- Learns addresses
- Receives BPDUs

Forwarding State

A Layer 2 interface in the forwarding state forwards frames. The interface enters the forwarding state from the learning state.

An interface in the forwarding state performs these functions:
- Receives and forwards frames received on the interface
- Forwards frames switched from another interface
- Learns addresses
- Receives BPDUs
Disabled State

A Layer 2 interface in the disabled state does not participate in frame forwarding or in the spanning tree. An interface in the disabled state is nonoperational.

A disabled interface performs these functions:

- Discards frames received on the interface
- Discards frames switched from another interface for forwarding
- Does not learn addresses
- Does not receive BPDUs

How a Switch or Port Becomes the Root Switch or Root Port

If all switches in a network are enabled with default spanning-tree settings, the switch with the lowest MAC address becomes the root switch. In Figure 16-2, Switch A is elected as the root switch because the switch priority of all the switches is set to the default (32768) and Switch A has the lowest MAC address. However, because of traffic patterns, number of forwarding interfaces, or link types, Switch A might not be the ideal root switch. By increasing the priority (lowering the numerical value) of the ideal switch so that it becomes the root switch, you force a spanning-tree recalculation to form a new topology with the ideal switch as the root.

![Spanning-Tree Topology](image)

When the spanning-tree topology is calculated based on default parameters, the path between source and destination end stations in a switched network might not be ideal. For instance, connecting higher-speed links to an interface that has a higher number than the root port can cause a root-port change. The goal is to make the fastest link the root port.

For example, assume that one port on Switch B is a Gigabit Ethernet link and that another port on Switch B (a 10/100 link) is the root port. Network traffic might be more efficient over the Gigabit Ethernet link. By changing the spanning-tree port priority on the Gigabit Ethernet port to a higher priority (lower numerical value) than the root port, the Gigabit Ethernet port becomes the new root port.
Spanning Tree and Redundant Connectivity

You can create a redundant backbone with spanning tree by connecting two switch interfaces to another device or to two different devices, as shown in Figure 16-3. Spanning tree automatically disables one interface but enables it if the other one fails. If one link is high-speed and the other is low-speed, the low-speed link is always disabled. If the speeds are the same, the port priority and port ID are added together, and spanning tree disables the link with the lowest value.

![Figure 16-3 Spanning Tree and Redundant Connectivity](image)

You can also create redundant links between switches by using EtherChannel groups. For more information, see the Chapter 35, “Configuring EtherChannels and Link-State Tracking.”

Spanning-Tree Address Management

IEEE 802.1D specifies 17 multicast addresses, ranging from 0x00180C2000000 to 0x0180C2000010, to be used by different bridge protocols. These addresses are static addresses that cannot be removed.

Regardless of the spanning-tree state, each switch receives but does not forward packets destined for addresses between 0x0180C2000000 and 0x0180C2000010.

If spanning tree is enabled, the CPU on the switch receives packets destined for 0x0180C2000000 and 0x0180C2000010. If spanning tree is disabled, the switch forwards those packets as unknown multicast addresses.

Accelerated Aging to Retain Connectivity

The default for aging dynamic addresses is 5 minutes, the default setting of the `mac-address-table aging-time` global configuration command. However, a spanning-tree reconfiguration 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 (spanning-tree vlan vlan-id forward-time seconds global configuration command) when the spanning tree reconfigures.
Because each VLAN is a separate spanning-tree instance, the switch accelerates aging on a per-VLAN basis. A spanning-tree reconfiguration 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.

**Spanning-Tree Modes and Protocols**

The switch supports these spanning-tree modes and protocols:

- **PVST+**—This spanning-tree mode is based on the IEEE 802.1D standard and Cisco proprietary extensions. It is the default spanning-tree mode used on all Ethernet, Fast Ethernet, and Gigabit Ethernet port-based VLANs. The PVST+ runs on each VLAN on the switch up to the maximum supported, ensuring that each has a loop-free path through the network.

  The PVST+ provides Layer 2 load balancing for the VLAN on which it runs. You can create different logical topologies by using the VLANs on your network to ensure that all of your links are used but that no one link is oversubscribed. Each instance of PVST+ on a VLAN has a single root switch. This root switch propagates the spanning-tree information associated with that VLAN to all other switches in the network. Because each switch has the same information about the network, this process ensures that the network topology is maintained.

- **Rapid PVST+**—This spanning-tree mode is the same as PVST+ except that it uses a rapid convergence based on the IEEE 802.1w standard. To provide rapid convergence, the rapid PVST+ immediately deletes dynamically learned MAC address entries on a per-port basis upon receiving a topology change. By contrast, PVST+ uses a short aging time for dynamically learned MAC address entries.

  The rapid PVST+ uses the same configuration as PVST+ (except where noted), and the switch needs only minimal extra configuration. The benefit of rapid PVST+ is that you can migrate a large PVST+ install base to rapid PVST+ without having to learn the complexities of the MSTP configuration and without having to reprovision your network. In rapid-PVST+ mode, each VLAN runs its own spanning-tree instance up to the maximum supported.

- **MSTP**—This spanning-tree mode is based on the IEEE 802.1s standard. You can map multiple VLANs to the same spanning-tree instance, which reduces the number of spanning-tree instances required to support a large number of VLANs. The MSTP runs on top of the RSTP (based on IEEE 802.1w), which provides for rapid convergence of the spanning tree by eliminating the forward delay and by quickly transitioning root ports and designated ports to the forwarding state. You cannot run MSTP without RSTP.

  The most common initial deployment of MSTP is in the backbone and distribution layers of a Layer 2 switched network. For more information, see Chapter 17, “Configuring MSTP.”

For information about the number of supported spanning-tree instances, see the next section.

**Supported Spanning-Tree Instances**

In PVST+ or rapid-PVST+ mode, the switch supports up to 128 spanning-tree instances.

In MSTP mode, the switch supports up to 65 MST instances. The number of VLANs that can be mapped to a particular MST instance is unlimited.

For information about how spanning tree interoperates with the VLAN Trunking Protocol (VTP), see the “Spanning-Tree Configuration Guidelines” section on page 16-12.
Spanning-Tree Interoperability and Backward Compatibility

Table 16-2 lists the interoperability and compatibility among the supported spanning-tree modes in a network.

<table>
<thead>
<tr>
<th>PVST+</th>
<th>MSTP</th>
<th>Rapid PVST+</th>
</tr>
</thead>
<tbody>
<tr>
<td>PVST+</td>
<td>Yes</td>
<td>Yes (with restrictions)</td>
</tr>
<tr>
<td>MSTP</td>
<td>Yes (with restrictions)</td>
<td>Yes</td>
</tr>
<tr>
<td>Rapid PVST+</td>
<td>Yes (reverts to PVST+)</td>
<td>Yes</td>
</tr>
</tbody>
</table>

In a mixed MSTP and PVST+ network, the common spanning-tree (CST) root must be inside the MST backbone, and a PVST+ switch cannot connect to multiple MST regions.

When a network contains switches running rapid PVST+ and switches running PVST+, we recommend that the rapid-PVST+ switches and PVST+ switches be configured for different spanning-tree instances. In the rapid-PVST+ spanning-tree instances, the root switch must be a rapid-PVST+ switch. In the PVST+ instances, the root switch must be a PVST+ switch. The PVST+ switches should be at the edge of the network.

STP and IEEE 802.1Q Trunks

The IEEE 802.1Q standard for VLAN trunks imposes some limitations on the spanning-tree strategy for a network. The standard requires only one spanning-tree instance for all VLANs allowed on the trunks. However, in a network of Cisco switches connected through IEEE 802.1Q trunks, the switches maintain one spanning-tree instance for each VLAN allowed on the trunks.

When you connect a Cisco switch to a non-Cisco device through an IEEE 802.1Q trunk, the Cisco switch uses PVST+ to provide spanning-tree interoperability. If rapid PVST+ is enabled, the switch uses it instead of PVST+. The switch combines the spanning-tree instance of the IEEE 802.1Q VLAN of the trunk with the spanning-tree instance of the non-Cisco IEEE 802.1Q switch.

However, all PVST+ or rapid-PVST+ information is maintained by Cisco switches separated by a cloud of non-Cisco IEEE 802.1Q switches. The non-Cisco IEEE 802.1Q cloud separating the Cisco switches is treated as a single trunk link between the switches.

PVST+ is automatically enabled on 802.1Q trunks, and no user configuration is required. The external spanning-tree behavior on access ports and Inter-Switch Link (ISL) trunk ports is not affected by PVST+.

For more information on 802.1Q trunks, see Chapter 11, “Configuring VLANs.”

VLAN-Bridge Spanning Tree

Cisco VLAN-bridge spanning tree is used with the fallback bridging feature (bridge groups), which forwards non-IP protocols such as DECnet between two or more VLAN bridge domains or routed ports. The VLAN-bridge spanning tree allows the bridge groups to form a spanning tree on top of the individual VLAN spanning trees to prevent loops from forming if there are multiple connections among VLANs. It also prevents the individual spanning trees from the VLANs being bridged from collapsing into a single spanning tree.
To support VLAN-bridge spanning tree, some of the spanning-tree timers are increased. To use the fallback bridging feature, you must have the enhanced multilayer software image installed on your switch. For more information, see Chapter 47, “Configuring Fallback Bridging.”

**Configuring Spanning-Tree Features**

These sections describe how to configure spanning-tree features:

- Default Spanning-Tree Configuration, page 16-11
- Spanning-Tree Configuration Guidelines, page 16-12
- Changing the Spanning-Tree Mode, page 16-13 (required)
- Disabling Spanning Tree, page 16-14 (optional)
- Configuring the Root Switch, page 16-14 (optional)
- Configuring a Secondary Root Switch, page 16-16 (optional)
- Configuring Port Priority, page 16-16 (optional)
- Configuring Path Cost, page 16-18 (optional)
- Configuring the Switch Priority of a VLAN, page 16-19 (optional)
- Configuring Spanning-Tree Timers, page 16-20 (optional)

**Default Spanning-Tree Configuration**

Table 16-3 shows the default spanning-tree configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable state</td>
<td>Enabled on VLAN 1. For more information, see the “Supported Spanning-Tree Instances” section on page 16-9.</td>
</tr>
<tr>
<td>Spanning-tree mode</td>
<td>PVST+. (Rapid PVST+ and MSTP are disabled.)</td>
</tr>
<tr>
<td>Switch priority</td>
<td>32768.</td>
</tr>
<tr>
<td>Spanning-tree port priority (configurable on a per-interface basis)</td>
<td>128.</td>
</tr>
</tbody>
</table>
| Spanning-tree port cost (configurable on a per-interface basis) | 1000 Mbps: 4.  
                          | 100 Mbps: 19.  
                          | 10 Mbps: 100.                                                               |
| Spanning-tree VLAN port priority (configurable on a per-VLAN basis) | 128.                                                                           |
Configuring Spanning-Tree Features

Table 16-3  Default Spanning-Tree Configuration (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spanning-tree VLAN port cost (configurable on a per-VLAN basis)</td>
<td>1000 Mbps: 4.</td>
</tr>
<tr>
<td></td>
<td>100 Mbps: 19.</td>
</tr>
<tr>
<td></td>
<td>10 Mbps: 100.</td>
</tr>
<tr>
<td>Spanning-tree timers</td>
<td>Hello time: 2 seconds.</td>
</tr>
<tr>
<td></td>
<td>Forward-delay time: 15 seconds.</td>
</tr>
<tr>
<td></td>
<td>Maximum-aging time: 20 seconds.</td>
</tr>
</tbody>
</table>

Spanning-Tree Configuration Guidelines

If more VLANs are defined in the VTP than there are spanning-tree instances, you can enable PVST+ or rapid PVST+ on only 128 VLANs on the switch. The remaining VLANs operate with spanning tree disabled. However, you can map multiple VLANs to the same spanning-tree instances by using MSTP. For more information, see Chapter 17, “Configuring MSTP.”

If 128 instances of spanning tree are already in use, you can disable spanning tree on one of the VLANs 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 spanning tree on a specific VLAN, and use the `spanning-tree vlan vlan-id` global configuration command to enable spanning tree 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 spanning-tree instance can break loops. Therefore, spanning tree must be running on enough switches to 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 spanning tree 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 already used all available spanning-tree instances on your switch, adding another VLAN anywhere in the VTP domain creates a VLAN that is not running spanning tree on that switch. 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 have all run out of spanning-tree instances. You can prevent this possibility by setting up allowed lists on the trunk ports of switches that have used up their allocation of spanning-tree instances. Setting up allowed lists is not necessary in many cases and can make it more labor-intensive to add another VLAN to the network.

Spanning-tree commands control the configuration of VLAN spanning-tree instances. You create a spanning-tree instance when you assign an interface to a VLAN. The spanning-tree instance is removed when the last interface is moved to another VLAN. You can configure switch and port parameters before a spanning-tree instance is created; these parameters are applied when the spanning-tree instance is created.
The switch supports PVST+, rapid PVST+, and MSTP, but only one version can be active at any time.
(For example, all VLANs run PVST+, all VLANs run rapid PVST+, or all VLANs run MSTP.) For
information about the different spanning-tree modes and how they interoperate, see the “Spanning-Tree Interoperability and Backward Compatibility” section on page 16-10.

For configuration guidelines about UplinkFast and BackboneFast, see the “Optional Spanning-Tree Configuration Guidelines” section on page 18-10.

### Changing the Spanning-Tree Mode

The switch supports three spanning-tree modes: PVST+, rapid PVST+, or MSTP. By default, the switch runs the PVST+ protocol.

Beginning in privileged EXEC mode, follow these steps to change the spanning-tree mode. If you want to enable a mode that is different from the default mode, this procedure is required.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
</tbody>
</table>
| **Step 2** | spanning-tree mode {pvst | mst | rapid-pvst} | Configure a spanning-tree mode.  
- Select **pvst** to enable PVST+ (the default setting).  
- Select **mst** to enable MSTP (and RSTP). For more configuration steps, see Chapter 17, “Configuring MSTP.”  
- Select **rapid-pvst** to enable rapid PVST+. |
| **Step 3** | interface interface-id | (Recommended for rapid-PVST+ mode only) Specify an interface to configure, and enter interface configuration mode. Valid interfaces include physical ports, VLANs, and port channels. The VLAN ID range is 1 to 4094. The port-channel range is 1 to 12. |
| **Step 4** | spanning-tree link-type point-to-point | (Recommended for rapid-PVST+ mode only) Specify that the link type for this port is point-to-point.  
If you connect this port (local port) to a remote port through a point-to-point link and the local port becomes a designated port, the switch negotiates with the remote port and rapidly transitions the local port to the forwarding state. |
| **Step 5** | end | Return to privileged EXEC mode. |
| **Step 6** | clear spanning-tree detected-protocols | (Recommended for rapid-PVST+ mode only) If any port on the switch is connected to a port on a legacy 802.1D switch, restart the protocol migration process on the entire switch.  
This step is optional if the designated switch detects that this switch is running rapid PVST+. |
| **Step 7** | show spanning-tree summary  
and  
show spanning-tree interface interface-id | Verify your entries. |
| **Step 8** | copy running-config startup-config | (Optional) Save your entries in the configuration file. |
To return to the default setting, use the **no spanning-tree mode** global configuration command. To return the port to its default setting, use the **no spanning-tree link-type** interface configuration command.

### Disabling Spanning Tree

Spanning tree is enabled by default on VLAN 1 and on all newly created VLANs up to the spanning-tree limit specified in the “Supported Spanning-Tree Instances” section on page 16-9. Disable spanning tree only if you are sure there are no loops in the network topology.

> **Caution**
>
> When spanning tree is disabled and loops are present in the topology, excessive traffic and indefinite packet duplication can drastically reduce network performance.

Beginning in privileged EXEC mode, follow these steps to disable spanning-tree on a per-VLAN basis. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>no spanning-tree vlan vlan-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
</tr>
<tr>
<td>Step 4</td>
<td>show spanning-tree vlan vlan-id</td>
</tr>
<tr>
<td>Step 5</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To re-enable spanning-tree, use the **spanning-tree vlan vlan-id** global configuration command.

### Configuring the Root Switch

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

To configure a switch to become the root for the specified VLAN, use the **spanning-tree vlan vlan-id root** global configuration command to modify the switch priority from the default value (32768) to a significantly lower value. When you enter this command, the software checks the switch priority of the root switches for each VLAN. Because of the extended system ID support, the switch sets its own priority for the specified VLAN to 24576 if this value will cause this switch to become the root for the specified VLAN.

If any root switch for the specified VLAN has a switch priority lower than 24576, the switch sets its own priority for the specified VLAN to 4096 less than the lowest switch priority. (4096 is the value of the least-significant bit of a 4-bit switch priority value as shown in Table 16-1 on page 16-4.)

> **Note**
>
> The **spanning-tree vlan vlan-id root** global configuration command fails if the value necessary to be the root switch is less than 1.
Chapter 16 Configuring STP

Configuring Spanning-Tree Features

### Note

If your network consists of switches that both do and do not support the extended system ID, it is unlikely that the switch with the extended system ID support will become the root switch. The extended system ID increases the switch priority value every time the VLAN number is greater than the priority of the connected switches running older software.

### Note

The root switch for each spanning-tree instance should be a backbone or distribution switch. Do not configure an access switch as the spanning-tree primary root.

Use the **diameter** keyword to specify the Layer 2 network diameter (that is, the maximum number of switch hops between any two end stations in the Layer 2 network). When you specify the network diameter, the switch automatically sets an optimal hello time, forward-delay time, and maximum-age time for a network of that diameter, which can significantly reduce the convergence time. You can use the **hello** keyword to override the automatically calculated hello time.

### Note

After configuring the switch as the root switch, we recommend that you avoid manually configuring the hello time, forward-delay time, and maximum-age time through the `spanning-tree vlan vlan-id hello-time`, `spanning-tree vlan vlan-id forward-time`, and the `spanning-tree vlan vlan-id max-age` global configuration commands.

Beginning in privileged EXEC mode, follow these steps to configure a switch to become the root for the specified VLAN. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>spanning-tree vlan vlan-id root primary [diameter net-diameter [hello-time seconds]]</code></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>end</code></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>show spanning-tree detail</code></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>copy running-config startup-config</code></td>
</tr>
</tbody>
</table>

To return to the default setting, use the **no spanning-tree vlan vlan-id root** global configuration command.
Configuring a Secondary Root Switch

When you configure the switch as the secondary root, the switch priority is modified from the default value (32768) to 28672. The switch is then likely to become the root switch for the specified VLAN if the primary root switch fails. This is assuming that the other network switches use the default switch priority of 32768 and therefore are unlikely to become the root switch.

You can execute this command on more than one switch to configure multiple backup root switches. Use the same network diameter and hello-time values that you used when you configured the primary root switch with the spanning-tree vlan vlan-id root primary global configuration command.

Beginning in privileged EXEC mode, follow these steps to configure a switch to become the secondary root for the specified VLAN. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>spanning-tree vlan vlan-id root secondary [diameter net-diameter [hello-time seconds]]</td>
</tr>
<tr>
<td></td>
<td>• For vlan-id, you can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) For diameter net-diameter, specify the maximum number of switches between any two end stations. The range is 2 to 7.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) For hello-time seconds, specify the interval in seconds between the generation of configuration messages by the root switch. The range is 1 to 10; the default is 2.</td>
</tr>
<tr>
<td></td>
<td>Use the same network diameter and hello-time values that you used when configuring the primary root switch. See the “Configuring the Root Switch” section on page 16-14.</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
</tr>
<tr>
<td>Step 4</td>
<td>show spanning-tree detail</td>
</tr>
<tr>
<td>Step 5</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To return to the default setting, use the no spanning-tree vlan vlan-id root global configuration command.

Configuring Port Priority

If a loop occurs, spanning tree uses the port priority when selecting an interface to put into the forwarding state. You can assign higher priority values (lower numerical values) to interfaces that you want selected first and lower priority values (higher numerical values) that you want selected last. If all interfaces have the same priority value, spanning tree puts the interface with the lowest interface number in the forwarding state and blocks the other interfaces.
Beginning in privileged EXEC mode, follow these steps to configure the port priority of an interface. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>spanning-tree port-priority priority</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>spanning-tree vlan vlan-id port-priority priority</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>show spanning-tree interface interface-id</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

**Note**

The show spanning-tree interface interface-id privileged EXEC command displays information only if the port is in a link-up operative state. Otherwise, you can use the show running-config interface privileged EXEC command to confirm the configuration.

To return to the default setting, use the no spanning-tree [vlan vlan-id] port-priority interface configuration command. For information on how to configure load sharing on trunk ports by using spanning-tree port priorities, see the “Configuring Trunk Ports for Load Sharing” section on page 11-23.
Configuring Path Cost

The spanning-tree path cost default value is derived from the media speed of an interface. If a loop occurs, spanning tree uses cost when selecting an interface to put in the forwarding state. You can assign lower cost values to interfaces that you want selected first and higher cost values that you want selected last. If all interfaces have the same cost value, spanning tree puts the interface with the lowest port number in the forwarding state and blocks the other interfaces.

Beginning in privileged EXEC mode, follow these steps to configure the cost of an interface. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><em>interface</em> interface-id Specify an interface to configure, and enter interface configuration mode. Valid interfaces include physical ports and port-channel logical interfaces (port-channel port-channel-number).</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><em>spanning-tree</em> cost cost Configure the cost for an interface. If a loop occurs, spanning tree uses the path cost when selecting an interface to place into the forwarding state. A lower path cost represents higher-speed transmission. For <em>cost</em>, the range is 1 to 200000000; the default value is derived from the media speed of the interface.</td>
</tr>
</tbody>
</table>
| **Step 4** | *spanning-tree* vlan vlan-id cost cost Configure the cost for a VLAN. If a loop occurs, spanning tree uses the path cost when selecting an interface to place into the forwarding state. A lower path cost represents higher-speed transmission.  
- For *vlan-id*, you can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.  
- For *cost*, the range is 1 to 200000000; the default value is derived from the media speed of the interface. |
| **Step 5** | end Return to privileged EXEC mode. |
| **Step 6** | show spanning-tree interface interface-id or show spanning-tree vlan vlan-id Verify your entries. |
| **Step 7** | copy running-config startup-config (Optional) Save your entries in the configuration file. |

>Note: The show spanning-tree interface interface-id privileged EXEC command displays information only for ports that are in a link-up operative state. Otherwise, you can use the show running-config privileged EXEC command to confirm the configuration.
To return to the default setting, use the **no spanning-tree** [vlan vlan-id] **cost** interface configuration command. For information on how to configure load sharing on trunk ports by using spanning-tree path costs, see the “Configuring Trunk Ports for Load Sharing” section on page 11-23.

## Configuring the Switch Priority of a VLAN

You can configure the switch priority and make it more likely that Catalyst 3750 Metro switch will be chosen as the root switch.

**Note**

Exercise care when using this command. For most situations, we recommend that you use the `spanning-tree vlan vlan-id root primary` and the `spanning-tree vlan vlan-id root secondary` global configuration commands to modify the switch priority.

Beginning in privileged EXEC mode, follow these steps to configure the switch priority of a VLAN. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>spanning-tree vlan vlan-id priority priority</td>
</tr>
<tr>
<td></td>
<td>• For <code>vlan-id</code>, you can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.</td>
</tr>
<tr>
<td></td>
<td>• For <code>priority</code>, the range is 0 to 61440 in increments of 4096; the default is 32768. The lower the number, the more likely the switch will be chosen as the root switch.</td>
</tr>
<tr>
<td></td>
<td>Valid priority values are 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>show spanning-tree vlan vlan-id</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To return to the default setting, use the **no spanning-tree vlan vlan-id priority** global configuration command.
Configuring Spanning-Tree Timers

Table 16-4 describes the timers that affect the entire spanning-tree performance.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hello timer</td>
<td>Controls how often the switch broadcasts hello messages to other switches.</td>
</tr>
<tr>
<td>Forward-delay timer</td>
<td>Controls how long each of the listening and learning states last before the interface begins forwarding.</td>
</tr>
<tr>
<td>Maximum-age timer</td>
<td>Controls the amount of time the switch stores protocol information received on an interface.</td>
</tr>
</tbody>
</table>

The sections that follow provide the configuration steps.

Configuring the Hello Time

You can configure the interval between the generation of configuration messages by the root switch by changing the hello time.

Exercise care when using this command. For most situations, we recommend that you use the `spanning-tree vlan vlan-id root primary` and the `spanning-tree vlan vlan-id root secondary` global configuration commands to modify the hello time.

Beginning in privileged EXEC mode, follow these steps to configure the hello time of a VLAN. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 spanning-tree vlan vlan-id hello-time seconds</td>
<td>Configure the hello time of a VLAN. The hello time is the interval between the generation of configuration messages by the root switch. These messages mean that the switch is alive.</td>
</tr>
<tr>
<td></td>
<td>• For <code>vlan-id</code>, you can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.</td>
</tr>
<tr>
<td></td>
<td>• For <code>seconds</code>, the range is 1 to 10; the default is 2.</td>
</tr>
<tr>
<td>Step 3 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4 show spanning-tree vlan vlan-id</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 5 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default setting, use the `no spanning-tree vlan vlan-id hello-time` global configuration command.
## Configuring the Forwarding-Delay Time for a VLAN

Beginning in privileged EXEC mode, follow these steps to configure the forwarding-delay time for a VLAN. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>spanning-tree vlan vlan-id forward-time seconds</td>
</tr>
<tr>
<td></td>
<td>Configure the forward time of a VLAN. The forward delay is the number of seconds an interface waits before changing from its spanning-tree learning and listening states to the forwarding state.</td>
</tr>
<tr>
<td></td>
<td>• For vlan-id, you can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.</td>
</tr>
<tr>
<td></td>
<td>• For seconds, the range is 4 to 30; the default is 15.</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
</tr>
<tr>
<td></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show spanning-tree vlan vlan-id</td>
</tr>
<tr>
<td></td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 5</td>
<td>copy running-config startup-config</td>
</tr>
<tr>
<td></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default setting, use the `no spanning-tree vlan vlan-id forward-time` global configuration command.

## Configuring the Maximum-Aging Time for a VLAN

Beginning in privileged EXEC mode, follow these steps to configure the maximum-aging time for a VLAN. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>spanning-tree vlan vlan-id max-age seconds</td>
</tr>
<tr>
<td></td>
<td>Configure the maximum-aging time of a VLAN. The maximum-aging time is the number of seconds a switch waits without receiving spanning-tree configuration messages before attempting a reconfiguration.</td>
</tr>
<tr>
<td></td>
<td>• For vlan-id, you can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.</td>
</tr>
<tr>
<td></td>
<td>• For seconds, the range is 6 to 40; the default is 20.</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
</tr>
<tr>
<td></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show spanning-tree vlan vlan-id</td>
</tr>
<tr>
<td></td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 5</td>
<td>copy running-config startup-config</td>
</tr>
<tr>
<td></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default setting, use the `no spanning-tree vlan vlan-id max-age` global configuration command.
Displaying the Spanning-Tree Status

To display the spanning-tree status, use one or more of the privileged EXEC commands in Table 16-5:

Table 16-5 Commands for Displaying Spanning-Tree Status

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show spanning-tree active</td>
<td>Displays spanning-tree information on active interfaces only.</td>
</tr>
<tr>
<td>show spanning-tree detail</td>
<td>Displays a detailed summary of interface information.</td>
</tr>
<tr>
<td>show spanning-tree interface interface-id</td>
<td>Displays spanning-tree information for the specified interface.</td>
</tr>
<tr>
<td>show spanning-tree summary [totals]</td>
<td>Displays a summary of interface states or displays the total lines of the STP state section.</td>
</tr>
</tbody>
</table>

You can clear spanning-tree counters by using the `clear spanning-tree [interface interface-id]` privileged EXEC command.

For information about other keywords for the `show spanning-tree` privileged EXEC command, see the command reference for this release.
CHAPTER 17

Configuring MSTP

This chapter describes how to configure the Cisco implementation of the IEEE 802.1s Multiple STP (MSTP) on the Catalyst 3750 Metro switch.

Note

The multiple spanning-tree (MST) implementation in Cisco IOS Release 12.2(25)SEG and later is based on the IEEE 802.1s standard. The MST implementations in earlier Cisco IOS releases are prestandard.

The MSTP enables multiple VLANs to be mapped to the same spanning-tree instance, thereby reducing the number of spanning-tree instances needed to support a large number of VLANs. The MSTP provides for multiple forwarding paths for data traffic and enables load balancing. It improves the fault tolerance of the network because a failure in one instance (forwarding path) does not affect other instances (forwarding paths). The most common initial deployment of MSTP is in the backbone and distribution layers of a Layer 2 switched network; this deployment provides the highly-available network required in a service-provider environment.

When the switch is in the multiple spanning-tree (MST) mode, the Rapid Spanning Tree Protocol (RSTP), which is based on IEEE 802.1w, is automatically enabled. The RSTP provides rapid convergence of the spanning tree through explicit handshaking that eliminates the IEEE 802.1D forwarding delay and quickly transitions root ports and designated ports to the forwarding state.

Both MSTP and RSTP improve the spanning-tree operation and maintain backward compatibility with equipment that is based on the (original) 802.1D spanning tree, with existing Cisco-proprietary Multiple Instance STP (MISTP), and with existing Cisco per-VLAN spanning-tree plus (PVST+) and rapid per-VLAN spanning-tree plus (rapid PVST+). For information about PVST+ and rapid PVST+, see Chapter 16, “Configuring STP.” For information about other spanning-tree features such as Port Fast, UplinkFast, root guard, and so forth, see Chapter 18, “Configuring Optional Spanning-Tree Features.”

Note

For complete syntax and usage information for the commands used in this chapter, see the command reference for this release.

This chapter consists of these sections:

- Understanding MSTP, page 17-2
- Understanding RSTP, page 17-8
- Configuring MSTP Features, page 17-13
- Displaying the MST Configuration and Status, page 17-26
Understanding MSTP

MSTP, which uses RSTP for rapid convergence, enables VLANs to be grouped into a spanning-tree instance, with each instance having a spanning-tree topology independent of other spanning-tree instances. This architecture provides multiple forwarding paths for data traffic, enables load balancing, and reduces the number of spanning-tree instances required to support a large number of VLANs.

These sections describe how the MSTP works:

- Multiple Spanning-Tree Regions, page 17-2
- IST, CIST, and CST, page 17-2
- Hop Count, page 17-5
- Boundary Ports, page 17-6
- IEEE 802.1s Implementation, page 17-6
- Interoperability with 802.1D STP, page 17-8

For configuration information, see the “Configuring MSTP Features” section on page 17-13.

Multiple Spanning-Tree Regions

For switches to participate in multiple spanning-tree (MST) instances, you must consistently configure the switches with the same MST configuration information. A collection of interconnected switches that have the same MST configuration comprises an MST region as shown in Figure 17-1 on page 17-4.

The MST configuration controls to which MST region each switch belongs. The configuration includes the name of the region, the revision number, and the MST VLAN-to-instance assignment map. You configure the switch for a region by using the `spanning-tree mst configuration` global configuration command, after which the switch enters the MST configuration mode. From this mode, you can map VLANs to an MST instance by using the `instance` MST configuration command, specify the region name by using the `name` MST configuration command, and set the revision number by using the `revision` MST configuration command.

A region can have one member or multiple members with the same MST configuration; each member must be capable of processing RSTP bridge protocol data units (BPDUs). There is no limit to the number of MST regions in a network, but each region can support up to 65 spanning-tree instances. Instances can be identified by any number in the range from 0 to 4094. You can assign a VLAN to only one spanning-tree instance at a time.

IST, CIST, and CST

Unlike PVST+ and rapid PVST+ in which all the spanning-tree instances are independent, the MSTP establishes and maintains two types of spanning trees:

- An internal spanning tree (IST), which is the spanning tree that runs in an MST region.

Within each MST region, the MSTP maintains multiple spanning-tree instances. Instance 0 is a special instance for a region, known as the internal spanning tree (IST). All other MST instances are numbered from 1 to 4094.
The IST is the only spanning-tree instance that sends and receives BPDUs; all of the other spanning-tree instance information is contained in M-records, which are encapsulated within MSTP BPDUs. Because the MSTP BPU carries information for all instances, the number of BPDUs that need to be processed by a switch to support multiple spanning-tree instances is significantly reduced.

All MST instances within the same region share the same protocol timers, but each MST instance has its own topology parameters, such as root switch ID, root path cost, and so forth. By default, all VLANs are assigned to the IST.

An MST instance is local to the region; for example, MST instance 1 in region A is independent of MST instance 1 in region B, even if regions A and B are interconnected.

- A common and internal spanning tree (CIST), which is a collection of the ISTs in each MST region, and the common spanning tree (CST) that interconnects the MST regions and single spanning trees.

The spanning tree computed in a region appears as a subtree in the CST that encompasses the entire switched domain. The CIST is formed as a result of the spanning-tree algorithm running between switches that support the 802.1w, 802.1s, and 802.1D protocols. The CIST inside an MST region is the same as the CST outside a region.

For more information, see the “Operations Within an MST Region” section on page 17-3 and the “Operations Between MST Regions” section on page 17-4.

Note

The implementation of the IEEE 802.1s standard changes some of the terminology associated with MST implementations. For a summary of these changes, see Table 17-1 on page 17-5.

Operations Within an MST Region

The IST connects all the MSTP switches in a region. When the IST converges, the root of the IST becomes the IST master (shown in Figure 17-1 on page 17-4), which is the switch within the region with the lowest bridge ID and path cost to the CST root. The IST master also is the CST root if there is only one region within the network. If the CST root is outside the region, one of the MSTP switches at the boundary of the region is selected as the IST master.

When an MSTP switch initializes, it sends BPDUs claiming itself as the root of the CST and the IST master, with both of the path costs to the CST root and to the IST master set to zero. The switch also initializes all of its MST instances and claims to be the root for all of them. If the switch receives superior MST root information (lower bridge ID, lower path cost, and so forth) than currently stored for the port, it relinquishes its claim as the IST master.

During initialization, a region might have many subregions, each with its own IST master. As switches receive superior IST information, they leave their old subregions and join the new subregion that might contain the true IST master. Thus all subregions shrink, except for the one that contains the true IST master.

For correct operation, all switches in the MST region must agree on the same IST master. Therefore, any two switches in the region synchronize their port roles for an MST instance only if they converge to a common IST master.
Operations Between MST Regions

If there are multiple regions or legacy 802.1D switches within the network, MSTP establishes and maintains the CST, which includes all MST regions and all legacy STP switches in the network. The MST instances combine with the IST at the boundary of the region to become the CST.

The IST connects all the MSTP switches in the region and appears as a subtree in the CST that encompasses the entire switched domain, with the root of the subtree being the IST master. The MST region appears as a virtual switch to adjacent STP switches and MST regions.

Figure 17-1 shows a network with three MST regions and a legacy 802.1D switch (D). The IST master for region 1 (A) is also the CST root. The IST master for region 2 (B) and the IST master for region 3 (C) are the roots for their respective subtrees within the CST. The RSTP runs in all regions.

Figure 17-1  MST Regions, IST Masters, and the CST Root

Figure 17-1 does not show additional MST instances for each region. Note that the topology of MST instances can be different from that of the IST for the same region.

Only the CST instance sends and receives BPDUs, and MST instances add their spanning-tree information into the BPDUs to interact with neighboring switches and compute the final spanning-tree topology. Because of this, the spanning-tree parameters related to BPDU transmission (for example, hello time, forward time, max-age, and max-hops) are configured only on the CST instance but affect all MST instances. Parameters related to the spanning-tree topology (for example, switch priority, port VLAN cost, port VLAN priority) can be configured on both the CST instance and the MST instance.

MSTP switches use Version 3 RSTP BPDUs or 802.1D STP BPDUs to communicate with legacy 802.1D switches. MSTP switches use MSTP BPDUs to communicate with MSTP switches.
IEEE 802.1s Terminology

Some MST naming conventions used in Cisco’s prestandard implementation have been changed to identify some internal or regional parameters. These parameters are significant only within an MST region, as opposed to external parameters that are relevant to the whole network. Because the CIST is the only spanning-tree instance that spans the whole network, only the CIST parameters require the external rather than the internal or regional qualifiers.

- The CIST root is the root switch for the unique instance that spans the whole network, the CIST.
- The CIST external root path cost is the cost to the CIST root. This cost is left unchanged within an MST region. Remember that an MST region looks like a single switch for the CIST. The CIST external root path cost is the root path cost calculated between these virtual switches and switches that do not belong to any region.
- The CIST regional root was called the IST master in the prestandard implementation. If the CIST root is in the region, the CIST regional root is the CIST root. Otherwise, the CIST regional root is the closest switch to the CIST root in the region. The CIST regional root acts as a root switch for the IST.
- The CIST internal root path cost is the cost to the CIST regional root in a region. This cost is only relevant to the IST, instance 0.

Table 17-1 compares the IEEE standard and the Cisco prestandard terminology.

### Table 17-1  Prestandard and Standard Terminology

<table>
<thead>
<tr>
<th>IEEE Standard</th>
<th>Cisco Prestandard</th>
<th>Cisco Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIST regional root</td>
<td>IST master</td>
<td>CIST regional root</td>
</tr>
<tr>
<td>CIST internal root path cost</td>
<td>IST master path cost</td>
<td>CIST internal path cost</td>
</tr>
<tr>
<td>CIST external root path cost</td>
<td>Root path cost</td>
<td>Root path cost</td>
</tr>
<tr>
<td>MSTI regional root</td>
<td>Instance root</td>
<td>Instance root</td>
</tr>
<tr>
<td>MSTI internal root path cost</td>
<td>Root path cost</td>
<td>Root path cost</td>
</tr>
</tbody>
</table>

**Hop Count**

The IST and MST instances do not use the message-age and maximum-age information in the configuration BPDU to compute the spanning-tree topology. Instead, they use the path cost to the root and a hop-count mechanism similar to the IP time-to-live (TTL) mechanism.

By using the `spanning-tree mst max-hops` global configuration command, you can configure the maximum hops inside the region and apply it to the IST and all MST instances in that region. The hop count achieves the same result as the message-age information (trigger a reconfiguration). The root switch of the instance always sends a BPDU (or M-record) with a cost of 0 and the hop count set to the maximum value. When a switch receives this BPDU, it decrements the received remaining hop count by one and propagates this value as the remaining hop count in the BPDUs it generates. When the count reaches zero, the switch discards the BPDU and ages the information held for the port.

The message-age and maximum-age information in the RSTP portion of the BPDU remain the same throughout the region, and the same values are propagated by the region’s designated ports at the boundary.
Boundary Ports

In the Cisco prestandard implementation, a boundary port connects an MST region to a single spanning-tree region running RSTP, to a single spanning-tree region running PVST+ or rapid PVST+, or to another MST region with a different MST configuration. A boundary port also connects to a LAN, the designated switch of which is either a single spanning-tree switch or a switch with a different MST configuration.

There is no definition of a boundary port in the IEEE 802.1s standard. The IEEE 802.1Q-2002 standard identifies two kinds of messages that a port can receive: internal (coming from the same region) and external. When a message is external, it is received only by the CIST. If the CIST role is root or alternate, or if the external BPDU is a topology change, it could have an impact on the MST instances. When a message is internal, the CIST part is received by the CIST, and each MST instance receives its respective M-record. The Cisco prestandard implementation treats a port that receives an external message as a boundary port. This means a port cannot receive a mix of internal and external messages.

An MST region includes both switches and LANs. A segment belongs to the region of its designated port. Therefore, a port in a different region than the designated port for a segment is a boundary port. This definition allows two ports internal to a region to share a segment with a port belonging to a different region, creating the possibility of receiving both internal and external messages on a port.

The primary change from the Cisco prestandard implementation is that a designated port is not defined as boundary, unless it is running in an STP-compatible mode.

Note

If there is a legacy STP switch on the segment, messages are always considered external.

The other change from the prestandard implementation is that the CIST regional root switch ID field is now inserted wherever an RSTP or legacy IEEE 802.1Q switch has the sender switch ID. The whole region performs like a single virtual switch by sending a consistent sender switch ID to neighboring switches. In this example, switch C would receive a BPDU with the same consistent sender switch ID of root, whether or not A or B is designated for the segment.

IEEE 802.1s Implementation

The Cisco implementation of the IEEE MST standard includes features required to meet the standard, as well as some of the desirable prestandard functionality that is not yet incorporated into the published standard.

Port Role Naming Change

The boundary role is no longer in the final MST standard, but this boundary concept is maintained in Cisco’s implementation. However, an MST instance port at a boundary of the region might not follow the state of the corresponding CIST port. Two cases exist now:

- The boundary port is the root port of the CIST regional root—When the CIST instance port is proposed and is in sync, it can send back an agreement and move to the forwarding state only after all the corresponding MSTI ports are in sync (and thus forwarding). The MSTI ports now have a special master role.
Understanding MSTP

The boundary port is not the root port of the CIST regional root—The MSTI ports follow the state and role of the CIST port. The standard provides less information, and it might be difficult to understand why an MSTI port can be alternately blocking when it receives no BPDUs (MRecords). In this case, although the boundary role no longer exists, the `show` commands identify a port as boundary in the `type` column of the output.

Interoperation Between Legacy and Standard Switches

Because automatic detection of prestandard switches can fail, you can use an interface configuration command to identify prestandard ports. A region cannot be formed between a standard and a prestandard switch, but they can interoperate by using the CIST. Only the capability of load balancing over different instances is lost in that particular case. The CLI displays different flags depending on the port configuration when a port receives prestandard BPDUs. A syslog message also appears the first time a switch receives a prestandard BPDU on a port that has not been configured for prestandard BPDU transmission.

Figure 17-2 illustrates this scenario. Assume that A is a standard switch and B a prestandard switch, both configured to be in the same region. A is the root switch for the CIST, and thus B has a root port (BX) on segment X and an alternate port (BY) on segment Y. If segment Y flaps, and the port on BY becomes the alternate before sending out a single prestandard BPDU, AY cannot detect that a prestandard switch is connected to Y and continues to send standard BPDUs. The port BY is thus fixed in a boundary, and no load balancing is possible between A and B. The same problem exists on segment X, but B might transmit topology changes.

Detecting Unidirectional Link Failure

This feature is not yet present in the IEEE MST standard, but it is included in this Cisco IOS release. The software checks the consistency of the port role and state in the received BPDUs to detect unidirectional link failures that could cause bridging loops.

When a designated port detects a conflict, it keeps its role, but reverts to discarding state because disrupting connectivity in case of inconsistency is preferable to opening a bridging loop.
Figure 17-3 illustrates a unidirectional link failure that typically creates a bridging loop. Switch A is the root switch, and its BPDUs are lost on the link leading to switch B. RSTP and MST BPDUs include the role and state of the sending port. With this information, switch A can detect that switch B does not react to the superior BPDUs it sends and that switch B is the designated, not root switch. As a result, switch A blocks (or keeps blocking) its port, thus preventing the bridging loop.

**Interoperability with 802.1D STP**

A switch running MSTP supports a built-in protocol migration mechanism that enables it to interoperate with legacy 802.1D switches. If this switch receives a legacy 802.1D configuration BPDU (a BPDU with the protocol version set to 0), it sends only 802.1D BPDUs on that port. An MSTP switch also can detect that a port is at the boundary of a region when it receives a legacy BPDU, an MSTP BPDU (Version 3) associated with a different region, or an RSTP BPDU (Version 2).

However, the switch does not automatically revert to the MSTP mode if it no longer receives 802.1D BPDUs. It cannot detect whether the legacy switch has been removed from the link unless the legacy switch is the designated switch. Also, a switch might continue to assign a boundary role to a port when the switch to which this switch is connected has joined the region. To restart the protocol migration process (force the renegotiation with neighboring switches), use the `clear spanning-tree detected-protocols` privileged EXEC command.

If all the legacy switches on the link are RSTP switches, they can process MSTP BPDUs as if they are RSTP BPDUs. Therefore, MSTP switches send either a Version 0 configuration and TCN BPDUs or Version 3 MSTP BPDUs on a boundary port. A boundary port connects to a LAN, the designated switch of which is either a single spanning-tree switch or a switch with a different MST configuration.

**Understanding RSTP**

The RSTP takes advantage of point-to-point wiring and provides rapid convergence of the spanning tree. Reconfiguration of the spanning tree can occur in less than 1 second (in contrast to 50 seconds with the default settings in the 802.1D spanning tree), which is critical for networks carrying delay-sensitive traffic such as voice and video.

These section describes how the RSTP works:

- **Port Roles and the Active Topology**, page 17-9
- **Rapid Convergence**, page 17-9
- **Synchronization of Port Roles**, page 17-11
- **Bridge Protocol Data Unit Format and Processing**, page 17-11

For configuration information, see the “Configuring MSTP Features” section on page 17-13.
Port Roles and the Active Topology

The RSTP provides rapid convergence of the spanning tree by assigning port roles and by learning the active topology. The RSTP builds upon the IEEE 802.1D STP to select the switch with the highest switch priority (lowest numerical priority value) as the root switch as described in the “Spanning-Tree Topology and BPDUs” section on page 16-3. Then the RSTP assigns one of these port roles to individual ports:

- **Root port**—Provides the best path (lowest cost) when the switch forwards packets to the root switch.
- **Designated port**—Connects to the designated switch, which incurs the lowest path cost when forwarding packets from that LAN to the root switch. The port through which the designated switch is attached to the LAN is called the designated port.
- **Alternate port**—Offers an alternate path toward the root switch to that provided by the current root port.
- **Backup port**—Acts as a backup for the path provided by a designated port toward the leaves of the spanning tree. A backup port can exist only when two ports are connected together in a loopback by a point-to-point link or when a switch has two or more connections to a shared LAN segment.
- **Disabled port**—Has no role within the operation of the spanning tree.

A port with the root or a designated port role is included in the active topology. A port with the alternate or backup port role is excluded from the active topology.

In a stable topology with consistent port roles throughout the network, the RSTP ensures that every root port and designated port immediately transition to the forwarding state while all alternate and backup ports are always in the discarding state (equivalent to blocking in 802.1D). The port state controls the operation of the forwarding and learning processes. Table 17-2 provides a comparison of 802.1D and RSTP port states.

<table>
<thead>
<tr>
<th>Operational Status</th>
<th>STP Port State (802.1D)</th>
<th>RSTP Port State</th>
<th>Is Port Included in the Active Topology?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Blocking</td>
<td>Discarding</td>
<td>No</td>
</tr>
<tr>
<td>Enabled</td>
<td>Listening</td>
<td>Discarding</td>
<td>No</td>
</tr>
<tr>
<td>Enabled</td>
<td>Learning</td>
<td>Learning</td>
<td>Yes</td>
</tr>
<tr>
<td>Enabled</td>
<td>Forwarding</td>
<td>Forwarding</td>
<td>Yes</td>
</tr>
<tr>
<td>Disabled</td>
<td>Disabled</td>
<td>Discarding</td>
<td>No</td>
</tr>
</tbody>
</table>

To be consistent with Cisco STP implementations, this guide documents the port state as **blocking** instead of **discarding**. Designated ports start in the listening state.

Rapid Convergence

The RSTP provides for rapid recovery of connectivity following the failure of a switch, a switch port, or a LAN. It provides rapid convergence for edge ports, new root ports, and ports connected through point-to-point links as follows:

- **Edge ports**—If you configure a port as an edge port on an RSTP switch by using the `spanning-tree portfast` interface configuration command, the edge port immediately transitions to the forwarding state. An edge port is the same as a Port Fast-enabled port, and you should enable it only on ports that connect to a single end station.
• Root ports—If the RSTP selects a new root port, it blocks the old root port and immediately transitions the new root port to the forwarding state.

• Point-to-point links—If you connect a port to another port through a point-to-point link and the local port becomes a designated port, it negotiates a rapid transition with the other port by using the proposal-agreement handshake to ensure a loop-free topology.

As shown in Figure 17-4, Switch A is connected to Switch B through a point-to-point link, and all of the ports are in the blocking state. Assume that the priority of Switch A is a smaller numerical value than the priority of Switch B. Switch A sends a proposal message (a configuration BPDU with the proposal flag set) to Switch B, proposing itself as the designated switch.

After receiving the proposal message, Switch B selects as its new root port the port from which the proposal message was received, forces all nonedge ports to the blocking state, and sends an agreement message (a BPDU with the agreement flag set) through its new root port.

After receiving Switch B’s agreement message, Switch A also immediately transitions its designated port to the forwarding state. No loops in the network are formed because Switch B blocked all of its nonedge ports and because there is a point-to-point link between Switches A and B.

When Switch C is connected to Switch B, a similar set of handshaking messages are exchanged. Switch C selects the port connected to Switch B as its root port, and both ends immediately transition to the forwarding state. With each iteration of this handshaking process, one more switch joins the active topology. As the network converges, this proposal-agreement handshaking progresses from the root toward the leaves of the spanning tree.

The switch learns the link type from the port duplex mode: a full-duplex port is considered to have a point-to-point connection; a half-duplex port is considered to have a shared connection. You can override the default setting that is controlled by the duplex setting by using the spanning-tree link-type interface configuration command.
Synchronization of Port Roles

When the switch receives a proposal message on one of its ports and that port is selected as the new root port, the RSTP forces all other ports to synchronize with the new root information.

The switch is synchronized with superior root information received on the root port if all other ports are synchronized. An individual port on the switch is synchronized if:

- That port is in the blocking state.
- It is an edge port (a port configured to be at the edge of the network).

If a designated port is in the forwarding state and is not configured as an edge port, it transitions to the blocking state when the RSTP forces it to synchronize with new root information. In general, when the RSTP forces a port to synchronize with root information and the port does not satisfy any of the above conditions, its port state is set to blocking.

After ensuring all of the ports are synchronized, the switch sends an agreement message to the designated switch corresponding to its root port. When the switches connected by a point-to-point link are in agreement about their port roles, the RSTP immediately transitions the port states to forwarding. The sequence of events is shown in Figure 17-5.

Bridge Protocol Data Unit Format and Processing

The RSTP BPDU format is the same as the IEEE 802.1D BPDU format except that the protocol version is set to 2. A new one-byte Version 1 Length field is set to zero, which means that no Version 1 protocol information is present. Table 17-3 shows the RSTP flag fields.
Understanding RSTP

The sending switch sets the proposal flag in the RSTP BPDU to propose itself as the designated switch on that LAN. The port role in the proposal message is always set to the designated port.

The sending switch sets the agreement flag in the RSTP BPDU to accept the previous proposal. The port role in the agreement message is always set to the root port.

The RSTP does not have a separate topology change notification (TCN) BPDU. It uses the topology change (TC) flag to show the topology changes. However, for interoperability with 802.1D switches, the RSTP switch processes and generates TCN BPDUs.

The learning and forwarding flags are set according to the state of the sending port.

Processing Superior BPDU Information

If a port receives superior root information (lower bridge ID, lower path cost, and so forth) than currently stored for the port, the RSTP triggers a reconfiguration. If the port is proposed and is selected as the new root port, RSTP forces all the other ports to synchronize.

If the BPDU received is an RSTP BPDU with the proposal flag set, the switch sends an agreement message after all of the other ports are synchronized. If the BPDU is an 802.1D BPDU, the switch does not set the proposal flag and starts the forward-delay timer for the port. The new root port requires twice the forward-delay time to transition to the forwarding state.

If the superior information received on the port causes the port to become a backup or alternate port, RSTP sets the port to the blocking state but does not send the agreement message. The designated port continues sending BPDUs with the proposal flag set until the forward-delay timer expires, at which time the port transitions to the forwarding state.

Processing Inferior BPDU Information

If a designated port receives an inferior BPDU (higher bridge ID, higher path cost, and so forth than currently stored for the port) with a designated port role, it immediately replies with its own information.

---

Table 17-3  RSTP BPDU Flags

<table>
<thead>
<tr>
<th>Bit</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Topology change (TC)</td>
</tr>
<tr>
<td>1</td>
<td>Proposal</td>
</tr>
<tr>
<td>2–3</td>
<td>Port role:</td>
</tr>
<tr>
<td>00</td>
<td>Unknown</td>
</tr>
<tr>
<td>01</td>
<td>Alternate port</td>
</tr>
<tr>
<td>10</td>
<td>Root port</td>
</tr>
<tr>
<td>11</td>
<td>Designated port</td>
</tr>
<tr>
<td>4</td>
<td>Learning</td>
</tr>
<tr>
<td>5</td>
<td>Forwarding</td>
</tr>
<tr>
<td>6</td>
<td>Agreement</td>
</tr>
<tr>
<td>7</td>
<td>Topology change acknowledgement (TCA)</td>
</tr>
</tbody>
</table>
Topography Changes

This section describes the differences between the RSTP and the 802.1D in handling spanning-tree topology changes.

- **Detection**—Unlike 802.1D in which *any* transition between the blocking and the forwarding state causes a topology change, *only* transitions from the blocking to the forwarding state cause a topology change with RSTP (only an increase in connectivity is considered a topology change). State changes on an edge port do not cause a topology change. When an RSTP switch detects a topology change, it flushes the learned information on all of its nonedge ports except on those from which it received the TC notification.

- **Notification**—Unlike 802.1D, which uses TCN BPDUs, the RSTP does not use them. However, for 802.1D interoperability, an RSTP switch processes and generates TCN BPDUs.

- **Acknowledgement**—When an RSTP switch receives a TCN message on a designated port from an 802.1D switch, it replies with an 802.1D configuration BPDU with the TCA bit set. However, if the TC-while timer (the same as the topology-change timer in 802.1D) is active on a root port connected to an 802.1D switch and a configuration BPDU with the TCA bit set is received, the TC-while timer is reset.

  This behavior is only required to support 802.1D switches. The RSTP BPDUs never have the TCA bit set.

- **Propagation**—When an RSTP switch receives a TC message from another switch through a designated or root port, it propagates the change to all of its nonedge, designated ports and to the root port (excluding the port on which it is received). The switch starts the TC-while timer for all such ports and flushes the information learned on them.

- **Protocol migration**—For backward compatibility with 802.1D switches, RSTP selectively sends 802.1D configuration BPDUs and TCN BPDUs on a per-port basis.

  When a port is initialized, the migrate-delay timer is started (specifies the minimum time during which RSTP BPDUs are sent), and RSTP BPDUs are sent. While this timer is active, the switch processes all BPDUs received on that port and ignores the protocol type.

  If the switch receives an 802.1D BPDU after the port’s migration-delay timer has expired, it assumes that it is connected to an 802.1D switch and starts using only 802.1D BPDUs. However, if the RSTP switch is using 802.1D BPDUs on a port and receives an RSTP BPDU after the timer has expired, it restarts the timer and starts using RSTP BPDUs on that port.

Configuring MSTP Features

These sections describe how to configure basic MSTP features:

- **Default MSTP Configuration**, page 17-14
- **MSTP Configuration Guidelines**, page 17-14
- **Specifying the MST Region Configuration and Enabling MSTP**, page 17-15 (required)
- **Configuring the Root Switch**, page 17-17 (optional)
- **Configuring a Secondary Root Switch**, page 17-18 (optional)
- **Configuring Port Priority**, page 17-19 (optional)
- **Configuring Path Cost**, page 17-20 (optional)
- **Configuring the Switch Priority**, page 17-21 (optional)
• Configuring the Hello Time, page 17-22 (optional)
• Configuring the Forwarding-Delay Time, page 17-23 (optional)
• Configuring the Maximum-Aging Time, page 17-23 (optional)
• Configuring the Maximum-Hop Count, page 17-24 (optional)
• Specifying the Link Type to Ensure Rapid Transitions, page 17-24 (optional)
• Designating the Neighbor Type, page 17-25 (optional)
• Restarting the Protocol Migration Process, page 17-25 (optional)

Default MSTP Configuration

Table 17-4 shows the default MSTP configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spanning-tree mode</td>
<td>PVST+ (Rapid PVST+ and MSTP are disabled).</td>
</tr>
<tr>
<td>Switch priority (configurable on a per-CIST port basis)</td>
<td>32768.</td>
</tr>
<tr>
<td>Spanning-tree port priority (configurable on a per-CIST port basis)</td>
<td>128.</td>
</tr>
<tr>
<td>Spanning-tree port cost (configurable on a per-CIST port basis)</td>
<td>1000 Mbps: 4.  100 Mbps: 19.  10 Mbps: 100.</td>
</tr>
<tr>
<td>Hello time</td>
<td>2 seconds.</td>
</tr>
<tr>
<td>Forward-delay time</td>
<td>15 seconds.</td>
</tr>
<tr>
<td>Maximum-aging time</td>
<td>20 seconds.</td>
</tr>
<tr>
<td>Maximum hop count</td>
<td>20 hops.</td>
</tr>
</tbody>
</table>

For information about the supported number of spanning-tree instances, see the “Supported Spanning-Tree Instances” section on page 16-9.

MSTP Configuration Guidelines

These are the configuration guidelines for MSTP:
• When you enable MST by using the `spanning-tree mode mst` global configuration command, RSTP is automatically enabled.
• For two or more switches to be in the same MST region, they must have the same VLAN-to-instance map, the same configuration revision number, and the same name.
• The switch supports up to 65 MST instances. The number of VLANs that can be mapped to a particular MST instance is unlimited.
PVST+, rapid PVST+, and MSTP are supported, but only one version can be active at any time. (For example, all VLANs run PVST+, all VLANs run rapid PVST+, or all VLANs run MSTP.) For more information, see the “Spanning-Tree Interoperability and Backward Compatibility” section on page 16-10. For information on the recommended trunk port configuration, see the “Interaction with Other Features” section on page 11-19.

VTP propagation of the MST configuration is not supported. However, you can manually configure the MST configuration (region name, revision number, and VLAN-to-instance mapping) on each switch within the MST region by using the command-line interface (CLI) or through the SNMP support.

For load balancing across redundant paths in the network to work, all VLAN-to-instance mapping assignments must match; otherwise, all traffic flows on a single link.

All MST boundary ports must be forwarding for load balancing between a PVST+ and an MST cloud or between a rapid-PVST+ and an MST cloud. For this to occur, the IST master of the MST cloud should also be the root of the CST. If the MST cloud consists of multiple MST regions, one of the MST regions must contain the CST root, and all of the other MST regions must have a better path to the root contained within the MST cloud than a path through the PVST+ or rapid-PVST+ cloud. You might have to manually configure the switches in the clouds.

Partitioning the network into a large number of regions is not recommended. However, if this situation is unavoidable, we recommend that you partition the switched LAN into smaller LANs interconnected by routers or non-Layer 2 devices.

For configuration guidelines about UplinkFast and BackboneFast, see the “Optional Spanning-Tree Configuration Guidelines” section on page 18-10.

Specifying the MST Region Configuration and Enabling MSTP

For two or more switches to be in the same MST region, they must have the same VLAN-to-instance mapping, the same configuration revision number, and the same name.

A region can have one member or multiple members with the same MST configuration; each member must be capable of processing RSTP BPDU. There is no limit to the number of MST regions in a network, but each region can support up to 65 spanning-tree instances. You can assign a VLAN to only one spanning-tree instance at a time.

Beginning in privileged EXEC mode, follow these steps to specify the MST region configuration and enable MSTP. This procedure is required.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 spanning-tree mst configuration</td>
<td>Enter MST configuration mode.</td>
</tr>
</tbody>
</table>
To return to the default MST region configuration, use the `no spanning-tree mst configuration` global configuration command. To return to the default VLAN-to-instance map, use the `no instance instance-id [vlan vlan-range]` MST configuration command. To return to the default name, use the `no name MST` configuration command. To return to the default revision number, use the `no revision MST` configuration command. To re-enable PVST+, use the `no spanning-tree mode` or the `spanning-tree mode pvst` global configuration command.

This example shows how to enter MST configuration mode, map VLANs 10 to 20 to MST instance 1, name the region `region1`, set the configuration revision to 1, display the pending configuration, apply the changes, and return to global configuration mode:

```
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# instance 1 vlan 10-20
Switch(config-mst)# name region1
Switch(config-mst)# revision 1
Switch(config-mst)# show pending
Pending MST configuration
Name      [region1]
Revision  1
```

---

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 3** | `instance instance-id vlan vlan-range` Map VLANs to an MST instance.  
  - For `instance-id`, the range is 0 to 4094.  
  - For `vlan vlan-range`, the range is 1 to 4094.  
  When you map VLANs to an MST instance, the mapping is incremental, and the VLANs specified in the command are added to or removed from the VLANs that were previously mapped.  
  To specify a VLAN range, use a hyphen; for example, `instance 1 vlan 1-63` maps VLANs 1 through 63 to MST instance 1.  
  To specify a VLAN series, use a comma; for example, `instance 1 vlan 10, 20, 30` maps VLANs 10, 20, and 30 to MST instance 1. |
| **Step 4** | `name name` Specify the configuration name. The `name` string has a maximum length of 32 characters and is case sensitive. |
| **Step 5** | `revision version` Specify the configuration revision number. The range is 0 to 65535. |
| **Step 6** | `show pending` Verify your configuration by displaying the pending configuration. |
| **Step 7** | `exit` Apply all changes, and return to global configuration mode. |
| **Step 8** | `spanning-tree mode mst` Enable MSTP. RSTP is also enabled.  
  **Caution** Changing spanning-tree modes can disrupt traffic because all spanning-tree instances are stopped for the previous mode and restarted in the new mode.  
  You cannot run both MSTP and PVST+ or both MSTP and rapid PVST+ at the same time. |
| **Step 9** | `end` Return to privileged EXEC mode. |
| **Step 10** | `show running-config` Verify your entries. |
| **Step 11** | `copy running-config startup-config` (Optional) Save your entries in the configuration file. |
Chapter 17  Configuring MSTP

Configuring MSTP Features

### Instance  Vlans Mapped

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1-9, 21-4094</td>
</tr>
<tr>
<td>1</td>
<td>10-20</td>
</tr>
</tbody>
</table>

Switch(config-mst)# exit
Switch(config)#

## Configuring the Root Switch

The switch maintains a spanning-tree instance for the group of VLANs mapped to it. A bridge ID, consisting of the switch priority and the switch MAC address, is associated with each instance. For a group of VLANs, the switch with the lowest bridge ID becomes the root switch.

To configure a switch to become the root, use the `spanning-tree mst instance-id root` global configuration command to modify the switch priority from the default value (32768) to a significantly lower value so that the switch becomes the root switch for the specified spanning-tree instance. When you enter this command, the switch checks the switch priorities of the root switches. Because of the extended system ID support, the switch sets its own priority for the specified instance to 24576 if this value will cause this switch to become the root for the specified spanning-tree instance.

If any root switch for the specified instance has a switch priority lower than 24576, the switch sets its own priority to 4096 less than the lowest switch priority. (4096 is the value of the least-significant bit of a 4-bit switch priority value as shown in Table 16-1 on page 16-4.)

If your network consists of switches that both do and do not support the extended system ID, it is unlikely that the switch with the extended system ID support will become the root switch. The extended system ID increases the switch priority value every time the VLAN number is greater than the priority of the connected switches running older software.

The root switch for each spanning-tree instance should be a backbone or distribution switch. Do not configure an access switch as the spanning-tree primary root.

Use the `diameter` keyword, which is available only for MST instance 0, to specify the Layer 2 network diameter (that is, the maximum number of switch hops between any two end stations in the Layer 2 network). When you specify the network diameter, the switch automatically sets an optimal hello time, forward-delay time, and maximum-age time for a network of that diameter, which can significantly reduce the convergence time. You can use the `hello` keyword to override the automatically calculated hello time.

**Note**

After configuring the switch as the root switch, we recommend that you avoid manually configuring the hello time, forward-delay time, and maximum-age time through the `spanning-tree mst hello-time`, `spanning-tree mst forward-time`, and the `spanning-tree mst max-age` global configuration commands.
Beginning in privileged EXEC mode, follow these steps to configure a switch as the root switch. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>spanning-tree mst instance-id root primary [diameter net-diameter [hello-time seconds]]</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>show spanning-tree mst instance-id</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To return the switch to its default setting, use the no spanning-tree mst instance-id root global configuration command.

**Configuring a Secondary Root Switch**

When you configure the switch with the extended system ID support as the secondary root, the switch priority is modified from the default value (32768) to 28672. The switch is then likely to become the root switch for the specified instance if the primary root switch fails. This is assuming that the other network switches use the default switch priority of 32768 and therefore are unlikely to become the root switch.

You can execute this command on more than one switch to configure multiple backup root switches. Use the same network diameter and hello-time values that you used when you configured the primary root switch with the spanning-tree mst instance-id root primary global configuration command.
Beginning in privileged EXEC mode, follow these steps to configure a switch as the secondary root switch. This procedure is optional.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>spanning-tree mst instance-id root secondary [diameter net-diameter [hello-time seconds]]</td>
<td>Configure a switch as the secondary root switch.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For instance-id, you can specify a single instance, a range of instances separated by a hyphen, or a series of instances separated by a comma. The range is 0 to 4094.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) For diameter net-diameter, specify the maximum number of switches between any two end stations. The range is 2 to 7. This keyword is available only for MST instance 0.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) For hello-time seconds, specify the interval in seconds between the generation of configuration messages by the root switch. The range is 1 to 10 seconds; the default is 2 seconds.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use the same network diameter and hello-time values that you used when configuring the primary root switch. See the “Configuring the Root Switch” section on page 17-17.</td>
</tr>
<tr>
<td>3</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>4</td>
<td>show spanning-tree mst instance-id</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>5</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return the switch to its default setting, use the no spanning-tree mst instance-id root global configuration command.

### Configuring Port Priority

If a loop occurs, the MSTP uses the port priority when selecting an interface to put into the forwarding state. You can assign higher priority values (lower numerical values) to interfaces that you want selected first and lower priority values (higher numerical values) that you want selected last. If all interfaces have the same priority value, the MSTP puts the interface with the lowest interface number in the forwarding state and blocks the other interfaces.

Beginning in privileged EXEC mode, follow these steps to configure the MSTP port priority of an interface. This procedure is optional.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>interface interface-id</td>
<td>Specify an interface to configure, and enter interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Valid interfaces include physical ports and port-channel logical interfaces. The port-channel range is 1 to 12.</td>
</tr>
</tbody>
</table>
Chapter 17  Configuring MSTP

Configuring MSTP Features

Note

The show spanning-tree mst interface interface-id privileged EXEC command displays information only if the port is in a link-up operative state. Otherwise, you can use the show running-config interface privileged EXEC command to confirm the configuration.

To return the interface to its default setting, use the no spanning-tree mst instance-id port-priority interface configuration command.

Configuring Path Cost

The MSTP path cost default value is derived from the media speed of an interface. If a loop occurs, the MSTP uses cost when selecting an interface to put in the forwarding state. You can assign lower cost values to interfaces that you want selected first and higher cost values that you want selected last. If all interfaces have the same cost value, the MSTP puts the interface with the lowest interface number in the forwarding state and blocks the other interfaces.

Beginning in privileged EXEC mode, follow these steps to configure the MSTP cost of an interface. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Specify an interface to configure, and enter interface configuration mode. Valid interfaces include physical ports and port-channel logical interfaces. The port-channel range is 1 to 12.</td>
</tr>
</tbody>
</table>
Chapter 17  Configuring MSTP

Configuring MSTP Features

Note
The show spanning-tree mst interface interface-id privileged EXEC command displays information only for interfaces that are in a link-up operative state. Otherwise, you can use the show running-config privileged EXEC command to confirm the configuration.

To return the interface to its default setting, use the no spanning-tree mst instance-id cost interface configuration command.

Configuring the Switch Priority

You can configure the switch priority and make it more likely that the switch will be chosen as the root switch.

Note
Exercise care when using this command. For most situations, we recommend that you use the spanning-tree mst instance-id root primary and the spanning-tree mst instance-id root secondary global configuration commands to modify the switch priority.
Beginning in privileged EXEC mode, follow these steps to configure the switch priority. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code> Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>spanning-tree mst instance-id priority priority</code> Configure the switch priority.</td>
</tr>
<tr>
<td></td>
<td>• For <code>instance-id</code>, you can specify a single instance, a range of instances separated by a hyphen, or a series of instances separated by a comma. The range is 0 to 4094.</td>
</tr>
<tr>
<td></td>
<td>• For <code>priority</code>, the range is 0 to 61440 in increments of 4096; the default is 32768. The lower the number, the more likely the switch will be chosen as the root switch.</td>
</tr>
<tr>
<td></td>
<td>Priority values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>end</code> Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>show spanning-tree mst instance-id</code> Verify your entries.</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>copy running-config startup-config</code> (Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return the switch to its default setting, use the `no spanning-tree mst instance-id priority` global configuration command.

### Configuring the Hello Time

You can configure the interval between the generation of configuration messages by the root switch by changing the hello time.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>spanning-tree mst hello-time seconds</code> Configure the hello time for all MST instances. The hello time is the interval between the generation of configuration messages by the root switch. These messages mean that the switch is alive. For <code>seconds</code>, the range is 1 to 10; the default is 2.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>end</code> Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

Exercise care when using this command. For most situations, we recommend that you use the `spanning-tree mst instance-id root primary` and the `spanning-tree mst instance-id root secondary` global configuration commands to modify the hello time.

Beginning in privileged EXEC mode, follow these steps to configure the hello time for all MST instances. This procedure is optional.
To return the switch to its default setting, use the `no spanning-tree mst hello-time` global configuration command.

### Configuring the Forwarding-Delay Time

Beginning in privileged EXEC mode, follow these steps to configure the forwarding-delay time for all MST instances. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><code>spanning-tree mst forward-time seconds</code></td>
<td>Configure the forward time for all MST instances. The forward delay is the number of seconds a port waits before changing from its spanning-tree learning and listening states to the forwarding state. For <code>seconds</code>, the range is 4 to 30; the default is 15.</td>
</tr>
<tr>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><code>show spanning-tree mst</code></td>
<td>Verify your entries.</td>
</tr>
<tr>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return the switch to its default setting, use the `no spanning-tree mst forward-time` global configuration command.

### Configuring the Maximum-Aging Time

Beginning in privileged EXEC mode, follow these steps to configure the maximum-aging time for all MST instances. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><code>spanning-tree mst max-age seconds</code></td>
<td>Configure the maximum-aging time for all MST instances. The maximum-aging time is the number of seconds a switch waits without receiving spanning-tree configuration messages before attempting a reconfiguration. For <code>seconds</code>, the range is 6 to 40; the default is 20.</td>
</tr>
<tr>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><code>show spanning-tree mst</code></td>
<td>Verify your entries.</td>
</tr>
<tr>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
To return the switch to its default setting, use the `no spanning-tree mst max-age` global configuration command.

### Configuring the Maximum-Hop Count

Beginning in privileged EXEC mode, follow these steps to configure the maximum-hop count for all MST instances. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 spanning-tree mst max-hops <code>hop-count</code></td>
<td>Specify the number of hops in a region before the BPDU is discarded, and the information held for a port is aged. For <code>hop-count</code>, the range is 1 to 255; the default is 20.</td>
</tr>
<tr>
<td>Step 3 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4 show spanning-tree mst</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 5 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return the switch to its default setting, use the `no spanning-tree mst max-hops` global configuration command.

### Specifying the Link Type to Ensure Rapid Transitions

If you connect a port to another port through a point-to-point link and the local port becomes a designated port, the RSTP negotiates a rapid transition with the other port by using the proposal-agreement handshake to ensure a loop-free topology as described in the “Rapid Convergence” section on page 17-9.

By default, the link type is controlled by the duplex mode of the port: a full-duplex port is considered to have a point-to-point connection; a half-duplex port is considered to have a shared connection. If you have a half-duplex link physically connected point-to-point to a single port on a remote switch running MSTP, you can override the default setting of the link type and enable rapid transitions to the forwarding state.

Beginning in privileged EXEC mode, follow these steps to override the default link-type setting. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface <code>interface-id</code></td>
<td>Specify the interface to configure, and enter interface configuration mode. Valid interfaces include physical port, VLANs, and port-channel logical interfaces. The VLAN ID range is 1 to 4094. The port-channel range is 1 to 12.</td>
</tr>
<tr>
<td>Step 3 spanning-tree link-type point-to-point</td>
<td>Specify that the link type of a port is point-to-point.</td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
Designating the Neighbor Type

A topology could contain both prestandard and IEEE 802.1s standard compliant devices. By default, ports can automatically detect prestandard devices, but they can still receive both standard and prestandard BPDUs. When there is a mismatch between a device and its neighbor, only the CIST runs on the interface.

You can choose to set a port to send only prestandard BPDUs. The prestandard flag appears in all the show commands, even if the port is in STP compatibility mode.

Beginning in privileged EXEC mode, follow these steps to override the default link-type setting. This procedure is optional.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>interface interface-id</td>
<td>Specify an interface to configure, and enter interface configuration mode. Valid interfaces include physical ports.</td>
</tr>
<tr>
<td>Step 4</td>
<td>spanning-tree mst pre-standard</td>
<td>Specify that the port can send only prestandard BPDUs.</td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 6</td>
<td>show spanning-tree mst interface interface-id</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 7</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return the port to its default setting, use the `no spanning-tree link-type` interface configuration command.

Restarting the Protocol Migration Process

A switch running MSTP supports a built-in protocol migration mechanism that enables it to interoperate with legacy 802.1D switches. If this switch receives a legacy 802.1D configuration BPDU (a BPDU with the protocol version set to 0), it sends only 802.1D BPDUs on that port. An MSTP switch also can detect that a port is at the boundary of a region when it receives a legacy BPDU, an MST BPDU (Version 3) associated with a different region, or an RST BPDU (Version 2).

However, the switch does not automatically revert to the MSTP mode if it no longer receives 802.1D BPDUs because it cannot detect whether the legacy switch has been removed from the link unless the legacy switch is the designated switch. A switch also might continue to assign a boundary role to a port when the switch to which it is connected has joined the region.

To restart the protocol migration process (force the renegotiation with neighboring switches) on the switch, use the `clear spanning-tree detected-protocols` privileged EXEC command.
To restart the protocol migration process on a specific port, use the `clear spanning-tree detected-protocols interface interface-id` privileged EXEC command.

### Displaying the MST Configuration and Status

To display the spanning-tree status, use one or more of the privileged EXEC commands in Table 17-5:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show spanning-tree mst configuration</code></td>
<td>Displays the MST region configuration.</td>
</tr>
<tr>
<td><code>show spanning-tree mst configuration digest</code></td>
<td>Displays the MD5 digest included in the current MSTCI.</td>
</tr>
<tr>
<td><code>show spanning-tree mst instance-id</code></td>
<td>Displays MST information for the specified instance.</td>
</tr>
<tr>
<td><code>show spanning-tree mst interface interface-id</code></td>
<td>Displays MST information for the specified interface.</td>
</tr>
</tbody>
</table>

For information about other keywords for the `show spanning-tree` privileged EXEC command, see the command reference for this release.
CHAPTER 18

Configuring Optional Spanning-Tree Features

This chapter describes how to configure optional spanning-tree features on the Catalyst 3750 Metro switch. You can configure all of these features when your switch is running the per-VLAN spanning-tree plus (PVST+). You can configure only the noted features when your switch is running the Multiple Spanning Tree Protocol (MSTP) or the rapid per-VLAN spanning-tree plus (rapid-PVST+) protocol.

For information on configuring the PVST+ and rapid PVST+, see Chapter 16, “Configuring STP.” For information about the Multiple Spanning Tree Protocol (MSTP) and how to map multiple VLANs to the same spanning-tree instance, see Chapter 17, “Configuring MSTP.”

For complete syntax and usage information for the commands used in this chapter, see the command reference for this release.

This chapter consists of these sections:

- Understanding Optional Spanning-Tree Features, page 18-1
- Configuring Optional Spanning-Tree Features, page 18-9
- Displaying the Spanning-Tree Status, page 18-16

Understanding Optional Spanning-Tree Features

These sections describe how the optional spanning-tree features work:

- Understanding Port Fast, page 18-2
- Understanding BPDU Guard, page 18-2
- Understanding BPDU Filtering, page 18-3
- Understanding UplinkFast, page 18-3
- Understanding BackboneFast, page 18-5
- Understanding EtherChannel Guard, page 18-7
- Understanding EtherChannel Guard, page 18-7
- Understanding Loop Guard, page 18-9
Understanding Port Fast

Port Fast immediately brings an interface configured as an access or trunk port to the forwarding state from a blocking state, bypassing the listening and learning states. You can use Port Fast on interfaces connected to a single workstation or server, as shown in Figure 18-1, to allow those devices to immediately connect to the network, rather than waiting for the spanning tree to converge.

Interfaces connected to a single workstation or server should not receive bridge protocol data units (BPDUs). An interface with Port Fast enabled goes through the normal cycle of spanning-tree status changes when the switch is restarted.

Note

Because the purpose of Port Fast is to minimize the time interfaces must wait for spanning-tree to converge, it is effective only when used on interfaces connected to end stations. If you enable Port Fast on an interface connecting to another switch, you risk creating a spanning-tree loop.

You can enable this feature by using the spanning-tree portfast interface configuration or the spanning-tree portfast default global configuration command.

Figure 18-1 Port Fast-Enabled Interfaces

Understanding BPDU Guard

The BPDU guard feature can be globally enabled on the switch or can be enabled per interface, but the feature operates with some differences.

At the global level, you enable BPDU guard on Port Fast-enabled interfaces by using the spanning-tree portfast bpduguard default global configuration command. Spanning tree shuts down interfaces that are in a Port Fast-operational state if any BPDU is received on those interfaces. In a valid configuration, Port Fast-enabled interfaces do not receive BPDUs. Receiving a BPDU on a Port Fast-enabled interface signals an invalid configuration, such as the connection of an unauthorized device, and the BPDU guard feature puts the interface in the error-disabled state.

At the interface level, you enable BPDU guard on any interface by using the spanning-tree bpduguard enable interface configuration command without also enabling the Port Fast feature. When the interface receives a BPDU, it is put in the error-disabled state.
The BPDU guard feature provides a secure response to invalid configurations because you must manually put the interface back in service. Use the BPDU guard feature in a service-provider network to prevent an access port from participating in the spanning tree.

You can enable the BPDU guard feature for the entire switch or for an interface.

### Understanding BPDU Filtering

The BPDU filtering feature can be globally enabled on the switch or can be enabled per interface, but the feature operates with some differences.

At the global level, you can enable BPDU filtering on Port Fast-enabled interfaces by using the `spanning-tree portfast bpdufilter default` global configuration command. This command prevents interfaces that are in a Port Fast-operational state from sending or receiving BPDUs. The interfaces still send a few BPDUs at link-up before the switch begins to filter outbound BPDUs. You should globally enable BPDU filtering on a switch so that hosts connected to these interfaces do not receive BPDUs. If a BPDU is received on a Port Fast-enabled interface, the interface loses its Port Fast-operational status, and BPDU filtering is disabled.

At the interface level, you can enable BPDU filtering on any interface by using the `spanning-tree bpdufilter enable` interface configuration command without also enabling the Port Fast feature. This command prevents the interface from sending or receiving BPDUs.

> **Caution**

Enabling BPDU filtering on an interface is the same as disabling spanning tree on it and can result in spanning-tree loops.

You can enable the BPDU filtering feature for the entire switch or for an interface.

### Understanding UplinkFast

Switches in hierarchical networks can be grouped into backbone switches, distribution switches, and access switches. Figure 18-2 shows a complex network where distribution switches and access switches each have at least one redundant link that spanning tree blocks to prevent loops.
If a switch loses connectivity, it begins using the alternate paths as soon as the spanning tree selects a new root port. By enabling UplinkFast with the `spanning-tree uplinkfast` global configuration command, you can accelerate the choice of a new root port when a link or switch fails or when the spanning tree reconfigures itself. The root port transitions to the forwarding state immediately without going through the listening and learning states, as it would with the normal spanning-tree procedures.

When the spanning tree reconfigures the new root port, other interfaces flood the network with multicast packets, one for each address that was learned on the interface. 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 spanning-tree topology converges more slowly after a loss of connectivity.

**Note**

UplinkFast is most useful in wiring-closet switches at the access or edge of the network. It is not appropriate for backbone devices. This feature might not be useful for other types of applications.

UplinkFast provides fast convergence after a direct link failure and achieves load balancing between redundant Layer 2 links using uplink groups. An uplink group is a set of Layer 2 ports (per VLAN), only one of which is forwarding at any given time. Specifically, an uplink group consists of the root port (which is forwarding) and a set of blocked ports, except for self-looping ports. The uplink group provides an alternate path in case the currently forwarding link fails.

**Figure 18-3** shows an example topology with no link failures. Switch A, the root switch, is connected directly to Switch B over link L1 and to Switch C over link L2. The Layer 2 interface on Switch C that is connected directly to Switch B is in a blocking state.
If Switch C detects a link failure on the currently active link L2 on the root port (a direct link failure), UplinkFast unblocks the blocked interface on Switch C and transitions it to the forwarding state without going through the listening and learning states, as shown in Figure 18-4. This change takes approximately 1 to 5 seconds.

**Understanding BackboneFast**

BackboneFast detects indirect failures in the core of the backbone. BackboneFast is a complementary technology to the UplinkFast feature, which responds to failures on links directly connected to access switches. BackboneFast optimizes the maximum-age timer, which controls the amount of time the switch stores protocol information received on an interface. When a switch receives an inferior BPDU from the designated port of another switch, the BPDU is a signal that the other switch might have lost its path to the root, and BackboneFast tries to find an alternate path to the root.

BackboneFast, which is enabled by using the `spanning-tree backbonefast` global configuration command, starts when a root port or blocked interface on a switch receives inferior BPDUs from its designated switch. An inferior BPDU identifies a switch that declares itself as both the root bridge and the designated switch. When a switch receives an inferior BPDU, it means that a link to which the switch is not directly connected (an indirect link) has failed (that is, the designated switch has lost its connection to the root switch). Under spanning-tree rules, the switch ignores inferior BPDUs for the configured maximum aging time specified by the `spanning-tree vlan vlan-id max-age` global configuration command.
The switch tries to determine if it has an alternate path to the root switch. If the inferior BPDU arrives on a blocked interface, the root port and other blocked interfaces on the switch become alternate paths to the root switch. (Self-looped ports are not considered alternate paths to the root switch.) If the inferior BPDU arrives on the root port, all blocked interfaces become alternate paths to the root switch. If the inferior BPDU arrives on the root port and there are no blocked interfaces, the switch assumes that it has lost connectivity to the root switch, causes the maximum aging time on the root port to expire, and becomes the root switch according to normal spanning-tree rules.

If the switch has alternate paths to the root switch, it uses these alternate paths to send a root link query (RLQ) request. The switch sends the RLQ request on all alternate paths and waits for an RLQ reply from other switches in the network.

If the switch discovers that it still has an alternate path to the root, it expires the maximum aging time on the interface that received the inferior BPDU. If all the alternate paths to the root switch indicate that the switch has lost connectivity to the root switch, the switch expires the maximum aging time on the interface that received the RLQ reply. If one or more alternate paths can still connect to the root switch, the switch makes all interfaces on which it received an inferior BPDU its designated ports and moves them from the blocking state (if they were in the blocking state), through the listening and learning states, and into the forwarding state.

Figure 18-5 shows an example topology with no link failures. Switch A, the root switch, connects directly to Switch B over link L1 and to Switch C over link L2. The Layer 2 interface on Switch C that connects directly to Switch B is in the blocking state.

If link L1 fails as shown in Figure 18-6, Switch C cannot detect this failure because it is not connected directly to link L1. However, because Switch B is directly connected to the root switch over L1, it detects the failure,elects itself the root, and begins sending BPDUs to Switch C, identifying itself as the root. When Switch C receives the inferior BPDUs from Switch B, Switch C assumes that an indirect failure has occurred. At that point, BackboneFast allows the blocked interface on Switch C to move immediately to the listening state without waiting for the maximum aging time for the interface to expire. BackboneFast then transitions the Layer 2 interface on Switch C to the forwarding state, providing a path from Switch B to Switch A. The root-switch election takes approximately 30 seconds, twice the Forward Delay time if the default Forward Delay time of 15 seconds is set. Figure 18-6 shows how BackboneFast reconfigures the topology to account for the failure of link L1.
Understanding Optional Spanning-Tree Features

If a new switch is introduced into a shared-medium topology as shown in Figure 18-7, BackboneFast is not activated because the inferior BPDUs did not come from the recognized designated switch (Switch B). The new switch begins sending inferior BPDUs that indicate it is the root switch. However, the other switches ignore these inferior BPDUs, and the new switch learns that Switch B is the designated switch to Switch A, the root switch.

Figure 18-7 Adding a Switch in a Shared-Medium Topology

Understanding EtherChannel Guard

You can use EtherChannel guard to detect an EtherChannel misconfiguration between the switch and a connected device. A misconfiguration can occur if the switch interfaces are configured in an EtherChannel, but the interfaces on the other device are not. A misconfiguration can also occur if the channel parameters are not the same at both ends of the EtherChannel. For EtherChannel configuration guidelines, see the “EtherChannel Configuration Guidelines” section on page 35-9.

If the switch detects a misconfiguration on the other device, EtherChannel guard places the switch interfaces in the error-disabled state, and displays an error message.

You can enable this feature by using the `spanning-tree etherchannel guard misconfig` global configuration command.
Understanding 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, the spanning tree can reconfigure itself and select a *customer switch* as the root switch, as shown in Figure 18-8. You can avoid this situation by enabling root guard on SP switch interfaces that connect to switches in your customer’s network. If spanning-tree calculations cause an interface in the customer network to be selected as the root port, root guard then places the interface in the root-inconsistent (blocked) state to prevent the customer’s switch from becoming the root switch or being in the path to the root.

If a switch outside the SP network becomes the root switch, the interface is blocked (root-inconsistent state), and spanning tree selects a new root switch. The customer’s switch does not become the root switch and is not in the path to the root.

If the switch is operating in multiple spanning-tree (MST) mode, root guard forces the interface to be a designated port. If a boundary port is blocked in an internal spanning-tree (IST) instance because of root guard, the interface also is blocked in all MST instances. A boundary port is an interface that connects to a LAN, the designated switch of which is either an 802.1D switch or a switch with a different MST region configuration.

Root guard enabled on an interface applies to all the VLANs to which the interface belongs. VLANs can be grouped and mapped to an MST instance.

You can enable this feature by using the `spanning-tree guard root` interface configuration command.

---

**Caution**

Misuse of the root-guard feature can cause a loss of connectivity.
Understanding Loop Guard

You can use loop guard to prevent alternate or root ports from becoming designated ports because of a failure that leads to a unidirectional link. This feature is most effective when it is enabled on the entire switched network. Loop guard prevents alternate and root ports from becoming designated ports, and spanning tree does not send BPDUs on root or alternate ports.

You can enable this feature by using the `spanning-tree loopguard default` global configuration command.

When the switch is operating in PVST+ or rapid-PVST+ mode, loop guard prevents alternate and root ports from becoming designated ports, and spanning tree does not send BPDUs on root or alternate ports.

When the switch is operating in MST mode, BPDUs are not sent on nonboundary ports only if the interface is blocked by loop guard in all MST instances. On a boundary port, loop guard blocks the interface in all MST instances.

Configuring Optional Spanning-Tree Features

These sections describe how to configure optional spanning-tree features:

- Default Optional Spanning-Tree Configuration, page 18-9
- Optional Spanning-Tree Configuration Guidelines, page 18-10
- Enabling Port Fast, page 18-10 (optional)
- Enabling BPDU Guard, page 18-11 (optional)
- Enabling BPDU Filtering, page 18-12 (optional)
- Enabling UplinkFast for Use with Redundant Links, page 18-13 (optional)
- Enabling BackboneFast, page 18-13 (optional)
- Enabling EtherChannel Guard, page 18-14 (optional)
- Enabling Root Guard, page 18-15 (optional)
- Enabling Loop Guard, page 18-15 (optional)

Default Optional Spanning-Tree Configuration

Table 18-1 shows the default optional spanning-tree configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Fast, BPDU filtering, BPDU guard</td>
<td>Globally disabled (unless they are individually configured per interface).</td>
</tr>
<tr>
<td>UplinkFast</td>
<td>Globally disabled.</td>
</tr>
<tr>
<td>BackboneFast</td>
<td>Globally disabled.</td>
</tr>
<tr>
<td>EtherChannel guard</td>
<td>Globally enabled.</td>
</tr>
<tr>
<td>Root guard</td>
<td>Disabled on all interfaces.</td>
</tr>
<tr>
<td>Loop guard</td>
<td>Disabled on all interfaces.</td>
</tr>
</tbody>
</table>
Optional Spanning-Tree Configuration Guidelines

You can configure PortFast, BPDU guard, BPDU filtering, EtherChannel guard, root guard, or loop guard if your switch is running PVST+, rapid PVST+, or MSTP.

You can configure the UplinkFast or the BackboneFast feature for rapid PVST+ or for the MSTP, but the feature remains disabled (inactive) until you change the spanning-tree mode to PVST+.

Enabling Port Fast

An interface with the Port Fast feature enabled moves directly to the spanning-tree forwarding state without waiting for the standard forward-time delay.

Caution

Use Port Fast only when connecting a single end station to an access or trunk port. Enabling this feature on an interface connected to a switch or hub could prevent spanning tree from detecting and disabling loops in your network, which could cause broadcast storms and address-learning problems.

If you enable the voice VLAN feature, the Port Fast feature is automatically enabled. When you disable voice VLAN, the Port Fast feature is not automatically disabled. For more information, see Chapter 14, “Configuring Voice VLAN.”

You can enable this feature if your switch is running PVST+, rapid PVST+, or MSTP.

Beginning in privileged EXEC mode, follow these steps to enable Port Fast. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>spanning-tree portfast [trunk]</td>
</tr>
<tr>
<td>Caution</td>
<td>Make sure that there are no loops in the network between the trunk port and the workstation or server before you enable Port Fast on a trunk port.</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
</tr>
<tr>
<td>Step 5</td>
<td>show spanning-tree interface interface-id portfast</td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

Note

You can use the spanning-tree portfast default global configuration command to globally enable the Port Fast feature on all nontrunking ports.
To disable the Port Fast feature, use the `spanning-tree portfast disable` interface configuration command.

### Enabling BPDU Guard

When you globally enable BPDU guard on ports that are Port Fast-enabled (the ports are in a Port Fast-operational state), spanning tree continues to run on the ports. They remain up unless they receive a BPDU.

In a valid configuration, Port Fast-enabled interfaces do not receive BPDUs. Receiving a BPDU on a Port Fast-enabled interface signals an invalid configuration, such as the connection of an unauthorized device, and the BPDU guard feature puts the interface in the error-disabled state. The BPDU guard feature provides a secure response to invalid configurations because you must manually put the interface back in service. Use the BPDU guard feature in a service-provider network to prevent an access port from participating in the spanning tree.

**Caution**
Configure Port Fast only on interfaces that connect to end stations; otherwise, an accidental topology loop could cause a data packet loop and disrupt switch and network operation.

You also can use the `spanning-tree bpduguard enable` interface configuration command to enable BPDU guard on any interface without also enabling the Port Fast feature. When the interface receives a BPDU, it is put in the error-disabled state.

You can enable the BPDU guard feature if your switch is running PVST+, rapid PVST+, or MSTP.

Beginning in privileged EXEC mode, follow these steps to globally enable the BPDU guard feature. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 spanning-tree portfast bpduguard default</td>
<td>Globally enable BPDU guard. By default, BPDU guard is disabled.</td>
</tr>
<tr>
<td>Step 3 <code>interface interface-id</code></td>
<td>Specify the interface connected to an end station, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 4 spanning-tree portfast</td>
<td>Enable the Port Fast feature.</td>
</tr>
<tr>
<td>Step 5 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 6 show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 7 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable BPDU guard, use the `no spanning-tree portfast bpduguard default` global configuration command.

You can override the setting of the `no spanning-tree portfast bpduguard default` global configuration command by using the `spanning-tree bpduguard enable` interface configuration command.
Enabling BPDU Filtering

When you globally enable BPDU filtering on Port Fast-enabled interfaces, it prevents interfaces that are in a Port Fast-operational state from sending or receiving BPDUs. The interfaces still send a few BPDUs at link-up before the switch begins to filter outbound BPDUs. You should globally enable BPDU filtering on a switch so that hosts connected to these interfaces do not receive BPDUs. If a BPU is received on a Port Fast-enabled interface, the interface loses its Port Fast-operational status, and BPDU filtering is disabled.

**Caution**
Configure Port Fast only on interfaces that connect to end stations; otherwise, an accidental topology loop could cause a data packet loop and disrupt switch and network operation.

You can also use the `spanning-tree bpdufilter enable` interface configuration command to enable BPDU filtering on any interface without also enabling the Port Fast feature. This command prevents the interface from sending or receiving BPDUs.

**Caution**
Enabling BPDU filtering on an interface is the same as disabling spanning tree on it and can result in spanning-tree loops.

You can enable the BPDU filtering feature if your switch is running PVST+, rapid PVST+, or MSTP. Beginning in privileged EXEC mode, follow these steps to globally enable the BPDU filtering feature. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code> Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>spanning-tree portfast bpdufilter default</code> Globally enable BPDU filtering. By default, BPDU filtering is disabled.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>interface interface-id</code> Specify the interface connected to an end station, and enter interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>spanning-tree portfast</code> Enable the Port Fast feature.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>end</code> Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>show running-config</code> Verify your entries.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><code>copy running-config startup-config</code> (Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable BPDU filtering, use the `no spanning-tree portfast bpdufilter default` global configuration command.

You can override the setting of the `no spanning-tree portfast bpdufilter default` global configuration command by using the `spanning-tree bpdufilter enable` interface configuration command.
Enabling UplinkFast for Use with Redundant Links

UplinkFast cannot be enabled on VLANs that have been configured with a switch priority. To enable UplinkFast on a VLAN with switch priority configured, first restore the switch priority on the VLAN to the default value by using the `no spanning-tree vlan vlan-id priority` global configuration command.

**Note**
When you enable UplinkFast, it affects all VLANs on the switch. You cannot configure UplinkFast on an individual VLAN.

You can configure the UplinkFast feature for rapid PVST+ or for MSTP, but the feature remains disabled (inactive) until you change the spanning-tree mode to PVST+.

Beginning in privileged EXEC mode, follow these steps to enable UplinkFast. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>spanning-tree uplinkfast [max-update-rate pkts-per-second]</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>show spanning-tree summary</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

When UplinkFast is enabled, the switch priority of all VLANs is set to 49152. If you change the path cost to a value less than 3000 and you enable UplinkFast or UplinkFast is already enabled, the path cost of all interfaces and VLAN trunks is increased by 3000 (if you change the path cost to 3000 or above, the path cost is not altered). The changes to the switch priority and the path cost reduce the chance that a switch will become the root switch.

When UplinkFast is disabled, the switch priorities of all VLANs and path costs of all interfaces are set to default values if you did not modify them from their defaults.

To return the update packet rate to the default setting, use the `no spanning-tree uplinkfast max-update-rate` global configuration command. To disable UplinkFast, use the `no spanning-tree uplinkfast` command.

Enabling BackboneFast

You can enable BackboneFast to detect indirect link failures and to start the spanning-tree reconfiguration sooner.

**Note**
If you use BackboneFast, you must enable it on all switches in the network. BackboneFast is not supported on Token Ring VLANs. This feature is supported for use with third-party switches.
You can configure the BackboneFast feature for rapid PVST+ or for MSTP, but the feature remains disabled (inactive) until you change the spanning-tree mode to PVST+.

Beginning in privileged EXEC mode, follow these steps to enable BackboneFast. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 spanning-tree backbonefast</td>
<td>Enable BackboneFast.</td>
</tr>
<tr>
<td>Step 3 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4 show spanning-tree summary</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 5 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable the BackboneFast feature, use the `no spanning-tree backbonefast` global configuration command.

### Enabling EtherChannel Guard

You can enable EtherChannel guard to detect an EtherChannel misconfiguration if your switch is running PVST+, rapid PVST+, or MSTP.

Beginning in privileged EXEC mode, follow these steps to enable EtherChannel guard. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 spanning-tree etherchannel guard misconfig</td>
<td>Enable EtherChannel guard.</td>
</tr>
<tr>
<td>Step 3 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4 show spanning-tree summary</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 5 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable the EtherChannel guard feature, use the `no spanning-tree etherchannel guard misconfig` global configuration command.

You can use the `show interfaces status err-disabled` privileged EXEC command to show which switch ports are disabled because of an EtherChannel misconfiguration. On the remote device, you can enter the `show etherchannel summary` privileged EXEC command to verify the EtherChannel configuration.

After the configuration is corrected, enter the `shutdown` and `no shutdown` interface configuration commands on the port-channel interfaces that were misconfigured.
Enabling Root Guard

Root guard enabled on an interface applies to all the VLANs to which the interface belongs. Do not enable the root guard on interfaces to be used by the UplinkFast feature. With UplinkFast, the backup interfaces (in the blocked state) replace the root port in the case of a failure. However, if root guard is also enabled, all the backup interfaces used by the UplinkFast feature are placed in the root-inconsistent state (blocked) and are prevented from reaching the forwarding state.

Note: You cannot enable both root guard and loop guard at the same time.

You can enable this feature if your switch is running PVST+, rapid PVST+, or MSTP.

Beginning in privileged EXEC mode, follow these steps to enable root guard on an interface. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td></td>
</tr>
<tr>
<td>interface interface-id</td>
<td>Specify an interface to configure, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td></td>
</tr>
<tr>
<td>spanning-tree guard root</td>
<td>Enable root guard on the interface. By default, root guard is disabled on all interfaces.</td>
</tr>
<tr>
<td>Step 4</td>
<td></td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5</td>
<td></td>
</tr>
<tr>
<td>show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 6</td>
<td></td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable root guard, use the `no spanning-tree guard` interface configuration command.

Enabling Loop Guard

You can use loop guard to prevent alternate or root ports from becoming designated ports because of a failure that leads to a unidirectional link. This feature is most effective when it is configured on the entire switched network. Loop guard operates only on interfaces that are considered point-to-point by the spanning tree.

Note: You cannot enable both loop guard and root guard at the same time.

You can enable this feature if your switch is running PVST+, rapid PVST+, or MSTP.

Beginning in privileged EXEC mode, follow these steps to enable loop guard. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td></td>
</tr>
<tr>
<td>show spanning-tree active or show spanning-tree mst</td>
<td>Verify which interfaces are alternate or root ports.</td>
</tr>
<tr>
<td>Step 2</td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
</tbody>
</table>
To globally disable loop guard, use the `no spanning-tree loopguard default` global configuration command. You can override the setting of the `no spanning-tree loopguard default` global configuration command by using the `spanning-tree guard loop` interface configuration command.

### Displaying the Spanning-Tree Status

To display the spanning-tree status, use one or more of the privileged EXEC commands in Table 18-2.

#### Table 18-2 Commands for Displaying the Spanning-Tree Status

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show spanning-tree active</td>
<td>Displays spanning-tree information on active interfaces only.</td>
</tr>
<tr>
<td>show spanning-tree detail</td>
<td>Displays a detailed summary of interface information.</td>
</tr>
<tr>
<td>show spanning-tree interface <code>interface-id</code></td>
<td>Displays spanning-tree information for the specified interface.</td>
</tr>
<tr>
<td>show spanning-tree mst interface <code>interface-id</code></td>
<td>Displays MST information for the specified interface.</td>
</tr>
<tr>
<td>show spanning-tree summary [totals]</td>
<td>Displays a summary of interface states or displays the total lines of the spanning-tree state section.</td>
</tr>
</tbody>
</table>

You can clear spanning-tree counters by using the `clear spanning-tree [interface interface-id]` privileged EXEC command.

For information about other keywords for the `show spanning-tree` privileged EXEC command, see the command reference for this release.
Configuring Resilient Ethernet Protocol

This chapter describes how to use Resilient Ethernet Protocol (REP) on the Catalyst 3750 Metro switch. REP is a Cisco proprietary protocol that provides an alternative to Spanning Tree Protocol (STP) to control network loops, handle link failures, and improve convergence time. REP controls a group of ports connected in a segment, ensures that the segment does not create any bridging loops, and responds to link failures within the segment. REP provides a basis for constructing more complex networks and supports VLAN load balancing.

This chapter includes these sections:
- Understanding REP, page 19-1
- Configuring REP, page 19-7
- Monitoring REP, page 19-15

Understanding REP

One REP segment is a chain of ports connected to each other and configured with a segment ID. Each segment consists of standard (non-edge) segment ports and two user-configured edge ports. A switch can have no more than two ports that belong to the same segment, and each segment port can have only one external neighbor. A segment can go through a shared medium, but on any link only two ports can belong to the same segment. REP is supported only on Layer 2 trunk interfaces.

Figure 19-1 shows an example of a segment consisting of six ports spread across four switches. Ports E1 and E2 are configured as edge ports. When all ports are operational (as in the segment on the left), a single port is blocked, shown by the diagonal line. When there is a failure in the network, as shown in the diagram on the right, the blocked port returns to the forwarding state to minimize network disruption.
**Figure 19-1** REP Open Segments

The segment shown in Figure 19-1 is an open segment; there is no connectivity between the two edge ports. The REP segment cannot cause a bridging loop and it is safe to connect the segment edges to any network. All hosts connected to switches inside the segment have two possible connections to the rest of the network through the edge ports, but only one connection is accessible at any time. If a failure causes a host to be unable to access its usual gateway, REP unblocks all ports to ensure that connectivity is available through the other gateway.

The segment shown in Figure 19-2, with both edge ports located on the same switch, is a ring segment. In this configuration, there is connectivity between the edge ports through the segment. With this configuration, you can create a redundant connection between any two switches in the segment.

**Figure 19-2** REP Ring Segment

REP segments have these characteristics:

- If all ports in the segment are operational, one port (referred to as the alternate port) is in the blocked state for each VLAN. If VLAN load balancing is configured, two ports in the segment control the blocked state of VLANs.
- If one or more ports in a segment is not operational, causing a link failure, all ports forward traffic on all VLANs to ensure connectivity.
- In case of a link failure, the alternate ports are unblocked as quickly as possible. When the failed link comes back up, a logically blocked port per VLAN is selected with minimal disruption to the network.
You can construct almost any type of network based on REP segments. REP also supports VLAN load-balancing, controlled by the primary edge port but occurring at any port in the segment.

In access ring topologies, the neighboring switch might not support REP, as shown in Figure 19-3. In this case, you can configure the non-REP facing ports (E1 and E2) as edge no-neighbor ports. These ports inherit all properties of edge ports, and you can configure them the same as any edge port, including configuring them to send STP or REP topology change notices to the aggregation switch. In this case the STP topology change notice (TCN) that is sent is a multiple spanning-tree (MST) STP message.

**Figure 19-3  Edge No-Neighbor Ports**

REP has these limitations:
- You must configure each segment port; an incorrect configuration can cause forwarding loops in the networks.
- REP can manage only a single failed port within the segment; multiple port failures within the REP segment cause loss of network connectivity.
- You should configure REP only in networks with redundancy. Configuring REP in a network without redundancy causes loss of connectivity.

**Link Integrity**

REP does not use an end-to-end polling mechanism between edge ports to verify link integrity. It implements local link failure detection. The REP Link Status Layer (LSL) detects its REP-aware neighbor and establishes connectivity within the segment. All VLANs are blocked on an interface until it detects the neighbor. After the neighbor is identified, REP determines which neighbor port should become the alternate port and which ports should forward traffic.

Each port in a segment has a unique port ID. The port ID format is similar to that used by the spanning tree algorithm: a port number (unique on the bridge), associated to a MAC address (unique in the network). When a segment port is coming up, its LSL starts sending packets that include the segment ID and the port ID. The port is declared as operational after it performs a three-way handshake with a neighbor in the same segment.
A segment port does not become operational if:

- No neighbor has the same segment ID.
- More than one neighbor has the same segment ID.
- The neighbor does not acknowledge the local port as a peer.

Each port creates an adjacency with its immediate neighbor. Once the neighbor adjacencies are created, the ports negotiate to determine one blocked port for the segment, the alternate port. All other ports become unblocked. By default, REP packets are sent to a BPDU class MAC address. The packets can also be sent to the Cisco multicast address, which is used only to send blocked port advertisement (BPA) messages when there is a failure in the segment. The packets are dropped by devices not running REP.

**Fast Convergence**

Because REP runs on a physical link basis and not a per-VLAN basis, only one hello message is required for all VLANs, reducing the load on the protocol. We recommend that you create VLANs consistently on all switches in a given segment and configure the same allowed VLANs on the REP trunk ports. To avoid the delay introduced by relaying messages in software, REP also allows some packets to be flooded to a regular multicast address. These messages operate at the hardware flood layer (HFL) and are flooded to the whole network, not just the REP segment. Switches that do not belong to the segment treat them as data traffic. You can control flooding of these messages by configuring a dedicated administrative VLAN for the whole domain.

The estimated convergence recovery time on fiber interfaces is less than 200 ms for the local segment with 200 VLANs configured. Convergence for VLAN load balancing is 300 ms or less.

**VLAN Load Balancing**

One edge port in the REP segment acts as the primary edge port; the other as the secondary edge port. It is the primary edge port that always participates in VLAN load balancing in the segment. REP VLAN balancing is achieved by blocking some VLANs at a configured alternate port and all other VLANs at the primary edge port. When you configure VLAN load balancing, you can specify the alternate port in one of three ways:

- By entering the port ID of the interface. To identify the port ID of a port in the segment, enter the `show interface rep detail` interface configuration command for the port.
- By entering the neighbor offset number of a port in the segment, which identifies the downstream neighbor port of an edge port. The neighbor offset number range is –256 to +256; a value of 0 is invalid. The primary edge port has an offset number of 1; positive numbers above 1 identify downstream neighbors of the primary edge port. Negative numbers indicate the secondary edge port (offset number -1) and its downstream neighbors.

*Note*

You configure offset numbers on the primary edge port by identifying a port’s downstream position from the primary (or secondary) edge port. You would never enter an offset value of 1 because that is the offset number of the primary edge port itself.

Figure 19-4 shows neighbor offset numbers for a segment where E1 is the primary edge port and E2 is the secondary edge port. The red numbers inside the ring are numbers offset from the primary edge port; the black numbers outside of the ring show the offset numbers from the secondary edge port. Note that you can identify all ports (except the primary edge port) by either a positive offset...
number (downstream position from the primary edge port) or a negative offset number (downstream position from the secondary edge port). If E2 became the primary edge port, its offset number would then be 1 and E1 would be -1.

- By entering the `preferred` keyword to select the port that you previously configured as the preferred alternate port with the `rep segment segment-id preferred` interface configuration command.

![Figure 19-4 Neighbor Offset Numbers in a Segment](image)

When the REP segment is complete, all VLANs are blocked. When you configure VLAN load balancing, you must also configure triggers in one of two ways:

- Manually trigger VLAN load balancing at any time by entering the `rep preempt segment segment-id` privileged EXEC command on the switch that has the primary edge port.
- Configure a preempt delay time by entering the `rep preempt delay seconds` interface configuration command. After a link failure and recovery, VLAN load balancing begins after the configured preemption time period elapses. Note that the delay timer restarts if another port fails before the time has elapsed.

**Note**

When VLAN load balancing is configured, it does not start working until triggered by either manual intervention or a link failure and recovery.

When VLAN load balancing is triggered, the primary edge port sends out a message to alert all interfaces in the segment about the preemption. When the secondary port receives the message, it is reflected into the network to notify the alternate port to block the set of VLANs specified in the message and to notify the primary edge port to block the remaining VLANs.

You can also configure a particular port in the segment to block all VLANs. Only the primary edge port initiates VLAN load balancing, which is not possible if the segment is not terminated by an edge port on each end. The primary edge port determines the local VLAN load balancing configuration.

Reconfigure the primary edge port to reconfigure load balancing. When you change the load balancing configuration, the primary edge port again waits for the `rep preempt segment` command or for the configured preempt delay period after a port failure and recovery before executing the new configuration. If you change an edge port to a regular segment port, the existing VLAN load balancing status does not change. Configuring a new edge port might cause a new topology configuration.
Note
Do not configure VLAN load balancing on an interface that carries Ethernet over multiprotocol label switching (EoMPLS) traffic. VLAN load balancing across the REP ring might prevent forwarding some of the EoMPLS traffic.

Spanning Tree Interaction

REP does not interact with STP or with the Flex Link feature, but can coexist with both. A port that belongs to a segment is removed from spanning tree control and STP BPDUs are not accepted or sent from segment ports. Therefore, STP cannot run on a segment.

To migrate from an STP ring configuration to REP segment configuration, begin by configuring a single port in the ring as part of the segment and continue by configuring contiguous ports to minimize the number of segments. Each segment always contains a blocked port, so multiple segments means multiple blocked ports and a potential loss of connectivity. When the segment has been configured in both directions up to the location of the edge ports, you then configure the edge ports.

REP Ports

Ports in REP segments are Failed, Open, or Alternate.
- A port configured as a regular segment port starts as a failed port.
- After the neighbor adjacencies are determined, the port transitions to alternate port state, blocking all VLANs on the interface. Blocked port negotiations occur and when the segment settles, one blocked port remains in the alternate role and all other ports become open ports.
- When a failure occurs in a link, all ports move to the failed state. When the alternate port receives the failure notification, it changes to the open state, forwarding all VLANs.

A regular segment port converted to an edge port, or an edge port converted to a regular segment port, does not always result in a topology change. If you convert an edge port into a regular segment port, VLAN load balancing is not implemented unless it has been configured. For VLAN load balancing, you must configure two edge ports in the segment.

A segment port that is reconfigured as a spanning tree port restarts according the spanning tree configuration. By default, this is a designated blocking port. If PortFast is configured or if STP is disabled, the port goes into the forwarding state.
Configuring REP

A segment is a collection of ports connected one to the other in a chain and configured with a segment ID. To configure REP segments, you configure the REP administrative VLAN (or use the default VLAN 1) and then add the ports to the segment using interface configuration mode. You should configure two edge ports in the segment, with one of them the primary edge port and the other by default the secondary edge port. A segment has only one primary edge port. If you configure two ports in a segment as the primary edge port, for example ports on different switches, the REP selects one of them to serve as the segment primary edge port. You can also optionally configure where to send segment topology change notices (STCNs) and VLAN load balancing.

- Default REP Configuration, page 19-7
- REP Configuration Guidelines, page 19-7
- Configuring the REP Administrative VLAN, page 19-9
- Configuring REP Interfaces, page 19-10
- Configuring SNMP Traps for REP, page 19-14

Default REP Configuration

REP is disabled on all interfaces. When enabled, the interface is a regular segment port unless it is configured as an edge port.

When REP is enabled, the sending of segment topology change notices (STCNs) is disabled, all VLANs are blocked, and the administrative VLAN is VLAN 1.

When VLAN load balancing is enabled, the default is manual preemption with the delay timer disabled. If VLAN load balancing is not configured, the default after manual preemption is to block all VLANs at the primary edge port.

REP Configuration Guidelines

Follow these guidelines when configuring REP:

- We recommend that you begin by configuring one port and then configure the contiguous ports to minimize the number of segments and the number of blocked ports.

- If more than two ports in a segment fail when no external neighbors are configured, one port changes to a forwarding state for the data path to help maintain connectivity during configuration. In the show rep interface privileged EXEC command output, the Port Role for this port shows as Fail Logical Open; the Port Role for the other failed port shows as Fail No Ext Neighbor. When the external neighbors for the failed ports are configured, the ports go through the alternate port state transitions and eventually go to an open state or remain as the alternate port, based on the alternate port election mechanism.

- REP ports must be Layer 2 trunk ports.

- Be careful when configuring REP through a Telnet connection. Because REP blocks all VLANs until another REP interface sends a message to unblock it, you might lose connectivity to the switch if you enable REP in a Telnet session that accesses the switch through the same interface.

- You cannot run REP and STP or REP and Flex Links on the same segment or interface.
• If you connect an STP network to the REP segment, be sure that the connection is at the segment edge. An STP connection that is not at the edge could cause a bridging loop because STP does not run on REP segments. All STP BPDUs are dropped at REP interfaces.

• You must configure all trunk ports in the segment with the same set of allowed VLANs, or a misconfiguration occurs.

• REP ports follow these rules:
  – There is no limit to the number of REP ports on a switch; however, only two ports on a switch can belong to the same REP segment.
  – If only one port on a switch is configured in a segment, the port should be an edge port.
  – If two ports on a switch belong to the same segment, they must be both edge ports, both regular segment ports, or one regular port and one edge no-neighbor port. An edge port and regular segment port on a switch cannot belong to the same segment.
  – If two ports on a switch belong to the same segment and one is configured as an edge port and one as a regular segment port (a misconfiguration), the edge port is treated as a regular segment port.

• REP interfaces come up in a blocked state and remains in a blocked state until notified that it is safe to unblock. You need to be aware of this to avoid sudden connection losses.

• REP sends all LSL PDUs in untagged frames on the native VLAN. The BPA message sent to the Cisco multicast address is sent on the administration VLAN, which is VLAN 1 by default.

• You can configure how long a REP interface remains up without receiving a hello from a neighbor. You can use the `rep isl-age-timer value` interface configuration command to set the time from 120 to 10000 ms. The LSL hello timer is then set to the age-timer value divided by 3. In normal operation, three LSL hellos are sent before the age timer on the peer switch expires and checks for hello messages.
  – In Cisco IOS Release 12.2(52)SE, the LSL age-timer range changes from 3000 to 10000 ms in 500-ms increments to 120 to 10000 ms in 40-ms increments. If the REP neighbor device is not running Cisco IOS Release 12.2(52) or later, you must use the shorter time range because the device does not accept values out of the earlier range.
  – EtherChannel port channel interfaces do not support LSL age-timer values less than 1000 ms. If you try to configure a value less than 1000 ms on a port channel, you receive an error message and the command is rejected.

• REP ports cannot be configured as one of these port types:
  – SPAN destination port
  – Private VLAN port
  – Tunnel port
  – Access port

• You should not configure VLAN load balancing on an interface that carries Ethernet over multiprotocol label switching (EoMPLS) traffic. VLAN load balancing across the REP ring might prevent forwarding some of the EoMPLS traffic.

• REP is supported on EtherChannels, but not on an individual port that belongs to an EtherChannel.

• There is a maximum of 64 REP segments per switch.
Configuring the REP Administrative VLAN

To avoid the delay introduced by relaying messages in software for link-failure or VLAN-blocking notification during load balancing, REP floods packets at the hardware flood layer (HFL) to a regular multicast address. These messages are flooded to the whole network, not just the REP segment. You can control flooding of these messages by configuring an administrative VLAN for the whole domain.

Follow these guidelines when configuring the REP administrative VLAN:

- If you do not configure an administrative VLAN, the default is VLAN 1.
- There can be only one administrative VLAN on a switch and on a segment. However, this is not enforced by software.
- The administrative VLAN cannot be the RSPAN VLAN.

Beginning in privileged EXEC mode, follow these steps to configure the REP administrative VLAN:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>rep admin vlan vlan-id</td>
<td>Specify the administrative VLAN. The range is 2 to 4094. The default is VLAN 1. To set the admin VLAN to 1, enter the no rep admin vlan global configuration command.</td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>show interface [interface-id] rep detail</td>
<td>Verify the configuration on one of the REP interfaces.</td>
</tr>
<tr>
<td>copy running-config startup config</td>
<td>(Optional) Save your entries in the switch startup configuration file.</td>
</tr>
</tbody>
</table>

This example shows how to configure the administrative VLAN as VLAN 100 and verify the configuration by entering the show interface rep detail command on one of the REP interfaces:

```
Switch# configure terminal
Switch (conf)# rep admin vlan 100
Switch (conf-if)# end

Switch# show interface gigabitethernet1/0/1 rep detail
GigabitEthernet1/0/1 REP enabled
Segment-id: 2 (Edge)
PortID: 00010019E7144680
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 0002001121A2D5800E4D
Port Role: Open
Blocked Vlan: <empty>
Admin-vlan: 100
Preempt Delay Timer: disabled
LSL Ageout Timer: 5000 ms
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none
LSL PDU rx: 3322, tx: 1722
HFL PDU rx: 32, tx: 5
BPA TLV rx: 16849, tx: 508
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
```
Configuring REP

For REP operation, you need to enable it on each segment interface and identify the segment ID. This step is required and must be done before other REP configuration. You must also configure a primary and secondary edge port on each segment. All other steps are optional.

Beginning in privileged EXEC mode, follow these steps to enable and configure REP on an interface:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Specify the interface, and enter interface configuration mode. The interface can be a physical Layer 2 interface or a port channel (logical interface). The port-channel range is 1 to 48.</td>
</tr>
<tr>
<td>Step 3 switchport mode trunk</td>
<td>Configure the interface as a Layer 2 trunk port.</td>
</tr>
<tr>
<td></td>
<td>On non-ES ports, you can also configure the encapsulation type by entering the switchport trunk encapsulation {isl</td>
</tr>
</tbody>
</table>
### Step 4
```
rep segment segment-id [edge [no-neighbor] [primary]] [preferred]
```

**Purpose**
Enable REP on the interface, and identify a segment number. The segment ID range is from 1 to 1024. These optional keywords are available.

**Note**
- You must configure two edge ports, including one primary edge port for each segment.
- Enter `edge` to configure the port as an edge port. Entering `edge` without the `primary` keyword configures the port as the secondary edge port. Each segment has only two edge ports.
- (Optional) On an edge port, enter `primary` to configure the port as the primary edge port, the port on which you can configure VLAN load balancing.
- (Optional) Enter `no-neighbor` to configure a port with no external REP neighbors as an edge port. The port inherits all properties of edge ports, and you can configure them the same as any edge port.

**Note**
Although each segment can have only one primary edge port, if you configure edge ports on two different switches and enter the `primary` keyword on both switches, the configuration is allowed. However, REP selects only one of these ports as the segment primary edge port. You can identify the primary edge port for a segment by entering the `show rep topology` privileged EXEC command.

- (Optional) Enter `preferred` to indicate that the port is the preferred alternate port or the preferred port for VLAN load balancing.

**Note**
Configuring a port as preferred does not guarantee that it becomes the alternate port; it merely gives it a slight edge among equal contenders. The alternate port is usually a previously failed port.

### Step 5
```
rep stcn {interface interface-id | segment id-list | stp}
```

(Optional) Configure the edge port to send segment topology change notices (STCNs).

- Enter `interface interface-id` to designate a physical interface or port channel to receive STCNs.
- Enter `segment id-list` to identify one or more segments to receive STCNs. The range is 1 to 1024.
- Enter `stp` to send STCNs to STP networks.
Step 6  
`rep block port {id port-id | neighbor_offset | preferred} vlan {vlan-list | all}`  
(Optional) Configure VLAN load balancing on the primary edge port, identify the REP alternate port in one of three ways, and configure the VLANs to be blocked on the alternate port.  
- Enter the `id port-id` to identify the alternate port by port ID. The port ID is automatically generated for each port in the segment. You can view interface port IDs by entering the `show interface interface-id rep [detail]` privileged EXEC command.  
- Enter a `neighbor_offset` number to identify the alternate port as a downstream neighbor from an edge port. The range is from –256 to 256, with negative numbers indicating the downstream neighbor from the secondary edge port. A value of 0 is invalid. Enter `-1` to identify the secondary edge port as the alternate port. See Figure 19-4 on page 19-5 for an example of neighbor offset numbering.  
- Enter `preferred` to select the regular segment port previously identified as the preferred alternate port for VLAN load balancing.  
- Enter `vlan vlan-list` to block one VLAN or a range of VLANs.  
- Enter `vlan all` to block all VLANs.  

Note  
Because you enter this command at the primary edge port (offset number 1), you would never enter an offset value of 1 to identify an alternate port.  
- Enter `preferred` to select the regular segment port previously identified as the preferred alternate port for VLAN load balancing.  
- Enter `vlan vlan-list` to block one VLAN or a range of VLANs.  
- Enter `vlan all` to block all VLANs.  

Note  
Enter this command only on the REP primary edge port.  

Step 7  
`rep preempt delay seconds`  
(Optional) You must enter this command and configure a preempt time delay if you want VLAN load balancing to automatically trigger after a link failure and recovery. The time delay range is 15 to 300 seconds. The default is manual preemption with no time delay.  

Note  
Enter this command only on the REP primary edge port.  

Step 8  
`rep isl-age-timer value`  
(Optional) Configure a time (in milliseconds) for which the REP interface remains up without receiving a hello from a neighbor. The range is from 120 to 10000 ms in 40-ms increments. The default is 5000 ms (5 seconds).  

Note  
If the neighbor device is not running Cisco IOS Release 12.2(52)SE or later, it only accepts values from 3000 to 10000 ms in 500-ms increments. EtherChannel port channel interfaces do not support LSL age-timer values less than 1000 ms.  

Step 9  
`end`  
Return to privileged EXEC mode.  

Step 10  
`show interface [interface-id] rep [detail]`  
Verify the REP interface configuration.  

Step 11  
`copy running-config startup config`  
(Optional) Save your entries in the switch startup configuration file.
Enter the `no` form of each command to return to the default configuration. Enter the `show rep topology` privileged EXEC command to see which port in the segment is the primary edge port.

This example shows how to configure an interface as the primary edge port for segment 1, to send STCNs to segments 2 through 5, and to configure the alternate port as the port with port ID 0009001818D68700 to block all VLANs after a preemption delay of 60 seconds after a segment port failure and recovery. The interface is configured to remain up for 6000 milliseconds without receiving a hello from a neighbor.

```
Switch# configure terminal
Switch (conf)# interface gigabitethernet1/0/1
Switch (conf-if)# rep segment 1 edge primary
Switch (conf-if)# rep stcn segment 2-5
Switch (conf-if)# rep block port 0009001818D68700 vlan all
Switch (conf-if)# rep preempt delay 60
Switch (conf-if)# rep isl-age-timer 6000
Switch (conf-if)# end
```

This example shows how to configure the same configuration when the interface has no external REP neighbor:

```
Switch# configure terminal
Switch (conf)# interface gigabitethernet1/0/1
Switch (conf-if)# rep segment 1 edge no-neighbor primary
Switch (conf-if)# rep stcn segment 2-5
Switch (conf-if)# rep block port 0009001818D68700 vlan all
Switch (conf-if)# rep preempt delay 60
Switch (conf-if)# rep isl-age-timer 6000
```

This example shows how to configure the VLAN blocking configuration shown in Figure 19-5. The alternate port is the neighbor with neighbor offset number 4. After manual preemption, VLANs 100 to 200 are blocked at this port, and all other VLANs are blocked at the primary edge port E1 (Gigabit Ethernet port 1/0/1).

```
Switch# configure terminal
Switch (conf)# interface gigabitethernet1/0/1
Switch (conf-if)# rep segment 1 edge primary
Switch (conf-if)# rep block port 4 vlan 100-200
Switch (conf-if)# end
```

**Figure 19-5 Example of VLAN Blocking**

![Figure 19-5 Example of VLAN Blocking](image_url)
Setting Manual Preemption for VLAN Load Balancing

If you do not enter the `rep preempt delay seconds` interface configuration command on the primary edge port to configure a preemption time delay, the default is to manually trigger VLAN load balancing on the segment. Be sure that all other segment configuration has been completed before manually preempting VLAN load balancing. When you enter the `rep preempt segment segment-id` command, a confirmation message appears before the command is executed because preemption can cause network disruption.

**Note**
Do not configure VLAN load balancing on an interface that carries Ethernet over multiprotocol label switching (EoMPLS) traffic. VLAN load balancing across the REP ring might prevent forwarding some of the EoMPLS traffic.

Beginning in privileged EXEC mode, follow these steps on the switch that has the segment primary edge port to manually trigger VLAN load balancing on a segment:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td></td>
</tr>
<tr>
<td><code>rep preempt segment segment-id</code></td>
<td>Manually trigger VLAN load balancing on the segment. You will need to confirm the command before it is executed.</td>
</tr>
<tr>
<td>Step 2</td>
<td></td>
</tr>
<tr>
<td><code>show rep topology</code></td>
<td>View REP topology information.</td>
</tr>
</tbody>
</table>

Configuring SNMP Traps for REP

You can configure the switch to send REP-specific traps to notify the SNMP server of link operational status changes and port role changes. Beginning in privileged EXEC mode, follow these steps to configure REP traps:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td></td>
</tr>
<tr>
<td><code>snmp mib rep trap-rate value</code></td>
<td>Enable the switch to send REP traps, and set the number of traps sent per second. The range is from 0 to 1000. The default is 0 (no limit imposed; a trap is sent at every occurrence).</td>
</tr>
<tr>
<td>Step 3</td>
<td></td>
</tr>
<tr>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td></td>
</tr>
<tr>
<td><code>show running-config</code></td>
<td>Verify the REP trap configuration.</td>
</tr>
<tr>
<td>Step 5</td>
<td></td>
</tr>
<tr>
<td><code>copy running-config startup config</code></td>
<td>(Optional) Save your entries in the switch startup configuration file.</td>
</tr>
</tbody>
</table>

To remove the trap, enter the `no snmp mib rep trap-rate` global configuration command.

This example configures the switch to send REP traps at a rate of 10 per second:

```
Switch(config)# snmp mib rep trap-rate 10
```
Monitoring REP

Use the privileged EXEC commands in Table 19-1 to monitor REP.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show interface [interface-id] rep [detail]</td>
<td>Displays REP configuration and status for an interface or for all interfaces.</td>
</tr>
<tr>
<td>show rep topology [segment segment_id] [archive] [detail]</td>
<td>Displays REP topology information for a segment or for all segments, including the primary and secondary edge ports in the segment.</td>
</tr>
</tbody>
</table>
Configuring Flex Links and the MAC Address-Table Move Update Feature

This chapter describes how to configure Flex Links, a pair of interfaces on the Catalyst 3750 Metro switch that provide a mutual backup. It also describes how to configure the MAC address-table move update feature, also referred to as the Flex Links bidirectional fast convergence feature.

Note

For complete syntax and usage information for the commands used in this chapter, see the command reference for this release.

The chapter consists of these sections:

- Understanding Flex Links and the MAC Address-Table Move Update, page 20-1
- Configuring Flex Links and MAC Address-Table Move Update, page 20-7
- Monitoring Flex Links and the MAC Address-Table Move Update, page 20-14

Understanding Flex Links and the MAC Address-Table Move Update

This section contains this information:

- Flex Links, page 20-1
- VLAN Flex Link Load Balancing and Support, page 20-2
- Flex Link Multicast Fast Convergence, page 20-3
- MAC Address-Table Move Update, page 20-6

Flex Links

Flex Links are a pair of a Layer 2 interfaces (switch ports or port channels) where one interface is configured to act as a backup to the other. The feature provides an alternative solution to the Spanning Tree Protocol (STP). Users can disable STP and still retain basic link redundancy. Flex Links are typically configured in service provider or enterprise networks where customers do not want to run STP on the switch. If the switch is running STP, Flex Links is not necessary because STP already provides link-level redundancy or backup.
You configure Flex Links on one Layer 2 interface (the active link) by assigning another Layer 2 interface as the Flex Link or backup link. When one of the links is up and forwarding traffic, the other link is in standby mode, ready to begin forwarding traffic if the other link shuts down. At any given time, only one of the interfaces is in the linkup state and forwarding traffic. If the primary link shuts down, the standby link starts forwarding traffic. When the active link comes back up, it goes into standby mode and does not forward traffic. STP is disabled on Flex Link interfaces.

In Figure 20-1, ports 1 and 2 on switch A are connected to uplink switches B and C. Because they are configured as Flex Links, only one of the interfaces is forwarding traffic; the other is in standby mode. If port 1 is the active link, it begins forwarding traffic between port 1 and switch B; the link between port 2 (the backup link) and switch C is not forwarding traffic. If port 1 goes down, port 2 comes up and starts forwarding traffic to switch C. When port 1 comes back up, it goes into standby mode and does not forward traffic; port 2 continues forwarding traffic.

You can also choose to configure a preemption mechanism, specifying the preferred port for forwarding traffic. In Figure 20-1, for example, you can configure the Flex Link pair with preemption mode so that after port 1 comes back up in the scenario, and it has greater bandwidth than port 2, port 1 begins forwarding after 60 seconds; and port 2 becomes the standby. You do this by entering the interface configuration `switchport backup interface preemption mode bandwidth` and `switchport backup interface preemption delay` commands.

If a primary (forwarding) link goes down, a trap notifies the network management stations. If the standby link goes down, a trap notifies the users.

Flex Links are supported only on Layer 2 ports and port channels, not on VLANs or on Layer 3 ports.

**VLAN Flex Link Load Balancing and Support**

VLAN Flex Link load-balancing allows users to configure a Flex Link pair so that both ports simultaneously forward the traffic for some mutually exclusive VLANs. For example, if Flex Link ports are configured for 1-100 VLANs, the traffic of the first 50 VLANs can be forwarded on one port and the rest on the other port. If one of the ports fail, the other active port forwards all the traffic. When the failed port comes back up, it resumes forwarding traffic in the preferred VLANs. This way, apart from providing the redundancy, this Flex Link pair can be used for load balancing. Also, Flex Link VLAN load-balancing does not impose any restrictions on uplink switches.
Flex Link Multicast Fast Convergence

Flex Link Multicast Fast Convergence reduces the multicast traffic convergence time after a Flex Link failure. This is implemented by a combination of these solutions:

- Learning the Other Flex Link Port as the mortar Port, page 20-3
- Generating IGMP Reports, page 20-3
- Leaking IGMP Reports, page 20-4

Learning the Other Flex Link Port as the mortar Port

In a typical multicast network, there is a querier for each VLAN. A switch deployed at the edge of a network has one of its Flex Link ports receiving queries. Flex Link ports are also always forwarding at any given time.

A port that receives queries is added as an *mrouter* port on the switch. An mrouter port is part of all the multicast groups learned by the switch. After a changeover, queries are received by the other Flex Link port. The other Flex Link port is then learned as the mrouter port. After changeover, multicast traffic then flows through the other Flex Link port. To achieve faster convergence of traffic, both Flex Link ports are learned as mrouter ports whenever either Flex Link port is learned as the mrouter port. Both Flex Link ports are always part of multicast groups.

Though both Flex Link ports are part of the groups in normal operation mode, all traffic on the backup port is blocked. So the normal multicast data flow is not affected by the addition of the backup port as an mrouter port. When the changeover happens, the backup port is unblocked, allowing the traffic to flow. In this case, the upstream multicast data flows as soon as the backup port is unblocked.

Generating IGMP Reports

When the backup link comes up after the changeover, the upstream new distribution switch does not start forwarding multicast data, because the port on the upstream router, which is connected to the blocked Flex Link port, is not part of any multicast group. The reports for the multicast groups were not forwarded by the downstream switch because the backup link is blocked. The data does not flow on this port, until it learns the multicast groups, which occurs only after it receives reports.

The reports are sent by hosts when a general query is received, and a general query is sent within 60 seconds in normal scenarios. When the backup link starts forwarding, to achieve faster convergence of multicast data, the downstream switch immediately sends proxy reports for all the learned groups on this port without waiting for a general query.
Leaking IGMP Reports

To achieve multicast traffic convergence with minimal loss, a redundant data path must be set up before the Flex Link active link goes down. This can be achieved by leaking only IGMP report packets on the Flex Link backup link. These leaked IGMP report messages are processed by upstream distribution routers, so multicast data traffic gets forwarded to the backup interface. Because all incoming traffic on the backup interface is dropped at the ingress of the access switch, no duplicate multicast traffic is received by the host. When the Flex Link active link fails, the access switch starts accepting traffic from the backup link immediately. The only disadvantage of this scheme is that it consumes bandwidth on the link between the distribution switches and on the backup link between the distribution and access switches. This feature is disabled by default and can be configured by using the `switchport backup interface interface-id multicast fast-convergence` command.

When this feature has been enabled at changeover, the switch does not generate the proxy reports on the backup port, which became the forwarding port.

Configuration Examples

These are configuration examples for learning the other Flex Link port as the mrouter port when Flex Link is configured on GigabitEthernet1/0/11 and GigabitEthernet1/0/12, and output for the `show interfaces switchport backup` command:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface GigabitEthernet1/0/11
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport backup interface Gi1/0/12
Switch(config-if)# exit
Switch(config)# interface GigabitEthernet1/0/12
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# end
Switch# show interfaces switchport backup detail
Switch Backup Interface Pairs:
   Active Interface Backup Interface State
   GigabitEthernet1/0/11 GigabitEthernet1/0/12 Active Up/Backup Standby
   Preemption Mode : off
   Multicast Fast Convergence : Off
   Bandwidth : 100000 Kbit (Gi1/0/11), 100000 Kbit (Gi1/0/12)
   Mac Address Move Update Vlan : auto
```

This output shows a querier for VLANs 1 and 401, with their queries reaching the switch through GigabitEthernet1/0/11:

```
Switch# show ip igmp snooping querier
Vlan IP Address IGMP Version Port
---------------------------------
1 1.1.1.1 v2 Gi1/0/11
401 41.41.41.1 v2 Gi1/0/11
```

Here is output for the `show ip igmp snooping mrouter` command for VLANs 1 and 401:

```
Switch# show ip igmp snooping mrouter
Vlan ports
----- -----        
1 Gi1/0/11(dynamiC), Gi1/0/12(dynamiC)
401 Gi1/0/11(dynamiC), Gi1/0/12(dynamiC)
```
Similarly, both Flex Link ports are part of learned groups. In this example, GigabitEthernet2/0/11 is a receiver/host in VLAN 1, which is interested in two multicast groups:

```
Switch# show ip igmp snooping groups
Vlan Group Type Version Port List
----------------- ------------------- --------------- ----------------------------------
1 228.1.5.1 igmp v2 Gi1/0/11, Gi1/0/12, Gi2/0/11
1 228.1.5.2 igmp v2 Gi1/0/11, Gi1/0/12, Gi2/0/11
```

When a host responds to the general query, the switch forwards this report on all the mrouter ports. In this example, when a host sends a report for the group 228.1.5.1, it is forwarded only on GigabitEthernet1/0/11, because the backup port GigabitEthernet1/0/12 is blocked. When the active link, GigabitEthernet1/0/11, goes down, the backup port, GigabitEthernet1/0/12, begins forwarding.

As soon as this port starts forwarding, the switch sends proxy reports for the groups 228.1.5.1 and 228.1.5.2 on behalf of the host. The upstream router learns the groups and starts forwarding multicast data. This is the default behavior of Flex Link. This behavior changes when the user configures fast convergence using the `switchport backup interface gigabitEthernet 1/0/12 multicast fast-convergence` command. This example shows turning on this feature:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitEthernet 1/0/11
Switch(config-if)# switchport backup interface gigabitEthernet 1/0/12 multicast fast-convergence
Switch(config-if)# exit
Switch# show interfaces switchport backup detail
Switch Backup Interface Pairs:
active Interface backup Interface state
GigabitEthernet1/0/11 GigabitEthernet1/0/12 Active Up/Backup Standby
Preemption Mode : off
Multicast Fast Convergence : On
Bandwidth : 100000 Kbit (Gi1/0/11), 100000 Kbit (Gi1/0/12)
Mac Address Move Update Vlan : auto
```

This output shows a querier for VLAN 1 and 401 with their queries reaching the switch through GigabitEthernet1/0/11:

```
Switch# show ip igmp snooping querier
Vlan IPv Address IGMP Version Port
----------------- --------------- -----
1 1.1.1.1 v2 Gi1/0/11
401 41.41.41.1 v2 Gi1/0/11
```

This is output for the `show ip igmp snooping mrouter` command for VLAN 1 and 401:

```
Switch# show ip igmp snooping mrouter
Vlan ports
----- -----
1 Gi1/0/11(dynamic), Gi1/0/12(dynamic)
401 Gi1/0/11(dynamic), Gi1/0/12(dynamic)
```

Similarly, both the Flex Link ports are a part of the learned groups. In this example, GigabitEthernet2/0/11 is a receiver/host in VLAN 1, which is interested in two multicast groups:

```
Switch# show ip igmp snooping groups
Vlan Group Type Version Port List
----------------- ------------------- --------------- ----------------------------------
1 228.1.5.1 igmp v2 Gi1/0/11, Gi1/0/12, Gi2/0/11
1 228.1.5.2 igmp v2 Gi1/0/11, Gi1/0/12, Gi2/0/11
```
Whenever a host responds to the General Query, the switch forwards this report on all the mrouter ports. When you turn on this feature through the command-line interface, when a report is forwarded by the switch on GigabitEthernet1/0/11, it is also leaked to the backup port GigabitEthernet1/0/12. The upstream router learns the groups and starts forwarding multicast data, which is dropped at the ingress because GigabitEthernet1/0/12 is blocked. When the active link, GigabitEthernet1/0/11, goes down, the backup port, GigabitEthernet1/0/12, begins forwarding. You do not need to send any proxy reports as the multicast data is already being forwarded by the upstream router. By leaking reports to the backup port, a redundant multicast path has been set up, and the time taken for the multicast traffic convergence is very minimal.

**MAC Address-Table Move Update**

The MAC address-table move update feature allows the switch to provide rapid bidirectional convergence when a primary (forwarding) link goes down and the standby link begins forwarding traffic.

In Figure 20-3, switch A is an access switch, and ports 1 and 2 on switch A are connected to uplink switches B and D through a Flex Link pair. Port 1 is forwarding traffic, and port 2 is in the backup state. Traffic from the PC to the server is forwarded from port 1 to port 3. The MAC address of the PC has been learned on port 3 of switch C. Traffic from the server to the PC is forwarded from port 3 to port 1.

If the MAC address-table move update feature is not configured and port 1 goes down, port 2 starts forwarding traffic. However, for a short time, switch C keeps forwarding traffic from the server to the PC through port 3, and the PC does not get the traffic because port 1 is down. If switch C removes the MAC address of the PC on port 3 and relearns it on port 4, traffic can then be forwarded from the server to the PC through port 2.

If the MAC address-table move update feature is configured and enabled on the switches in Figure 20-3 and port 1 goes down, port 2 starts forwarding traffic from the PC to the server. The switch sends a MAC address-table move update packet from port 2. Switch C gets this packet on port 4 and immediately learns the MAC address of the PC on port 4, which reduces the reconvergence time.

You can configure the access switch, switch A, to send MAC address-table move update messages. You can also configure the uplink switches B, C, and D to get and process the MAC address-table move update messages. When switch C gets a MAC address-table move update message from switch A, switch C learns the MAC address of the PC on port 4. Switch C updates the MAC address table, including the forwarding table entry for the PC.

Switch A does not need to wait for the MAC address-table update. The switch detects a failure on port 1 and immediately starts forwarding server traffic from port 2, the new forwarding port. This change occurs in 100 milliseconds (ms). The PC is directly connected to switch A, and the connection status does not change. Switch A does not need to update the PC entry in the MAC address table.
Configuring Flex Links and MAC Address-Table Move Update

These sections contain this information:

- Default Configuration, page 20-8
- Configuration Guidelines, page 20-8
- Configuring Flex Links, page 20-9
- Configuring VLAN Load Balancing on Flex Links, page 20-11
- Configuring the MAC Address-Table Move Update Feature, page 20-12
Default Configuration

The Flex Links are not configured, and there are no backup interfaces defined.
The preemption mode is off.
The preemption delay is 35 seconds.
Flex Link VLAN load balancing is not configured.
The MAC address-table move update feature is not configured on the switch.

Configuration Guidelines

Follow these guidelines to configure Flex Links:

- You can configure up to 16 backup links.
- You can configure only one Flex Link backup link for any active link, and it must be a different interface from the active interface.
- An interface can belong to only one Flex Link pair. An interface can be a backup link for only one active link. An active link cannot belong to another Flex Link pair.
- Neither of the links can be a port that belongs to an EtherChannel. However, you can configure two port channels (EtherChannel logical interfaces) as Flex Links, and you can configure a port channel and a physical interface as Flex Links, with either the port channel or the physical interface as the active link.
- A backup link does not have to be the same type (Fast Ethernet, Gigabit Ethernet, or port channel) as the active link. However, you should configure both Flex Links with similar characteristics so that there are no loops or changes in behavior if the standby link begins to forward traffic.
- STP is disabled on Flex Link ports. A Flex Link port does not participate in STP, even if the VLANs present on the port are configured for STP. When STP is not enabled, be sure that there are no loops in the configured topology.

Follow these guidelines to configure VLAN load balancing on the Flex Links feature:

- For Flex Link VLAN load balancing, you must choose the preferred VLANs on the backup interface.
- You cannot configure a preemption mechanism and VLAN load balancing for the same Flex Links pair.

Follow these guidelines to configure MAC address-table move update feature:

- You can enable and configure this feature on the access switch to send the MAC address-table move updates.
- You can enable and configure this feature on the uplink switches to get the MAC address-table move updates.
Configuring Flex Links

Beginning in privileged EXEC mode, follow these steps to configure a pair of Flex Links:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Specify the interface, and enter interface configuration mode. The interface can be a physical Layer 2 interface or a port channel (logical interface). The port-channel range is 1 to 48.</td>
</tr>
<tr>
<td>Step 3 switchport backup interface interface-id</td>
<td>Configure a physical Layer 2 interface (or port channel) as part of a Flex Link pair with the interface. When one link is forwarding traffic, the other interface is in standby mode.</td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5 show interface [interface-id] switchport backup</td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td>Step 6 copy running-config startup config</td>
<td>(Optional) Save your entries in the switch startup configuration file.</td>
</tr>
</tbody>
</table>

To disable a Flex Link backup interface, use the no switchport backup interface interface-id interface configuration command.

This example shows how to configure an interface with a backup interface and to verify the configuration:

```
Switch# configure terminal
Switch(conf)# interface fastethernet1/0/1
Switch(conf-if)# switchport backup interface fastethernet1/0/2
Switch(conf-if)# end
Switch# show interface switchport backup
Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------------------------
FastEthernet1/0/1       FastEthernet1/0/2       Active Up/Backup Standby
FastEthernet1/0/3       FastEthernet1/0/4       Active Up/Backup Standby
Port-channel1           GigabitEthernet1/0/1    Active Up/Backup Standby
```

Beginning in privileged EXEC mode, follow these steps to configure a preemption scheme for a pair of Flex Links:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Specify the interface, and enter interface configuration mode. The interface can be a physical Layer 2 interface or a port channel (logical interface). The port-channel range is 1 to 48.</td>
</tr>
</tbody>
</table>
### Configuring Flex Links and the MAC Address-Table Move Update Feature

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong> switchport backup interface interface-id</td>
<td>Configure a physical Layer 2 interface (or port channel) as part of a Flex Link pair with the interface. When one link is forwarding traffic, the other interface is in standby mode.</td>
</tr>
</tbody>
</table>
| **Step 4** switchport backup interface interface-id preemption mode [forced | bandwidth | off] | Configure a preemption mechanism and delay for a Flex Link interface pair. You can configure the preemption mode as:  
- **forced**—the active interface always preempts the backup  
- **bandwidth**—the interface with higher bandwidth always acts as the active interface  
- **off**—no preemption happens from active to backup |
| **Step 5** switchport backup interface interface-id preemption delay delay-time | Configure the delay time until a port preempts another port.  
**Note** Setting a delay time only works with forced and bandwidth modes. |
| **Step 6** end | Return to privileged EXEC mode. |
| **Step 7** show interface [interface-id] switchport backup | Verify the configuration. |
| **Step 8** copy running-config startup config | (Optional) Save your entries in the switch startup configuration file. |

To remove a preemption scheme, use the **no switchport backup interface interface-id preemption mode** interface configuration command. To reset the delay time to the default, use the **no switchport backup interface interface-id preemption delay** interface configuration command.

This example shows how to configure preemption mode as bandwidth, for a backup interface pair and to verify the configuration:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# switchport backup interface gigabitethernet1/0/2
Switch(config-if)# switchport backup interface gigabitethernet1/0/2 preemption mode forced
Switch(config-if)# switchport backup interface gigabitethernet1/0/2 preemption delay 50
Switch(config-if)# end
Switch# show interface switchport backup detail
Active Interface Backup Interface State
GigabitEthernet1/0/21 GigabitEthernet1/0/2 Active Down/Backup Down
Interface Pair : Gi1/0/21, Gi1/0/2
Preemption Mode : forced
Preemption Delay : 50 seconds
Bandwidth : 10000 Kbit (Gi1/0/1), 10000 Kbit (Gi1/0/2)
Mac Address Move Update Vlan : auto
<output truncated>
```
Chapter 20 Configuring Flex Links and the MAC Address-Table Move Update Feature

Configuring VLAN Load Balancing on Flex Links

Beginning in privileged EXEC mode, follow these steps to configure VLAN load balancing on Flex Links:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>switchport backup interface interface-id prefer vlan vlan-range</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
</tr>
<tr>
<td>Step 5</td>
<td>show interfaces [interface-id] switchport backup</td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup config</td>
</tr>
</tbody>
</table>

To disable the VLAN load balancing feature, use the no switchport backup interface interface-id prefer vlan vlan-range interface configuration command.

In this example, VLANs 1 to 50, 60, and 100 to 120 are configured on the switch:

```
Switch(config)# interface fastEthernet 1/0/6
Switch(config-if)# switchport backup interface fastEthernet 1/0/8 prefer vlan 60,100-120
```

When both interfaces are up, Fast Ethernet port 1/0/8 forwards traffic for VLANs 60 and 100 to 120 and Fast Ethernet port 1/0/6 forwards traffic for VLANs 1 to 50.

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:
  Active Interface        Backup Interface        State
  -------------------------------------------------------------------
  FastEthernet2/0/6    FastEthernet1/0/8        Active Up/Backup Standby

Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120
```

When a Flex Link interface goes down (LINK_DOWN), VLANs preferred on this interface are moved to the peer interface of the Flex Link pair. In this example, if interface 1/0/6 goes down, interface 1/0/8 carries all VLANs of the Flex Link pair.

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:
  Active Interface        Backup Interface        State
  -------------------------------------------------------------------
  FastEthernet2/0/6    FastEthernet2/0/8        Active Down/Backup Up

Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120
```
When a Flex Link interface comes up, VLANs preferred on this interface are blocked on the peer interface and moved to the forwarding state on the interface that has just come up. In this example, if interface Fast Ethernet port 1/0/6 comes up, VLANs preferred on this interface are blocked on the peer interface Fast Ethernet port 1/0/8 and forwarded on Fast Ethernet port 1/0/6.

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:
Active Interface        Backup Interface        State
------------------------------------------------------------------------
FastEthernet2/0/6    FastEthernet2/0/8    Active Up/Backup Standby
Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120
```

```
Switch# show interfaces switchport backup detail
Switch Backup Interface Pairs:
Active Interface        Backup Interface        State
------------------------------------------------------------------------
FastEthernet1/0/3       FastEthernet1/0/4       Active Down/Backup Up
Vlans Preferred on Active Interface: 1-2,5-4094
Vlans Preferred on Backup Interface: 3-4
Preemption Mode : off
Bandwidth : 10000 Kbit (Fa1/0/3), 100000 Kbit (Fa1/0/4)
Mac Address Move Update Vlan : auto
```

### Configuring the MAC Address-Table Move Update Feature

This section contains this information:

- Configuring a switch to send MAC address-table move updates
- Configuring a switch to get MAC address-table move updates

Beginning in privileged EXEC mode, follow these steps to configure an access switch to send MAC address-table move updates:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Enter global configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Specify the interface, and enter interface configuration mode. The interface can be a physical Layer 2 interface or a port channel (logical interface). The port-channel range is 1 to 48.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>switchport backup interface interface-id</td>
</tr>
<tr>
<td>Configure a physical Layer 2 interface (or port channel), as part of a Flex Link pair with the interface. The MAC address-table move update VLAN is the lowest VLAN ID on the interface.</td>
<td></td>
</tr>
<tr>
<td>or switchport backup interface interface-id mmu primary vlan vlan-id</td>
<td></td>
</tr>
<tr>
<td>Configure a physical Layer 2 interface (or port channel) and specify the VLAN ID on the interface, which is used for sending the MAC address-table move update.</td>
<td></td>
</tr>
<tr>
<td>When one link is forwarding traffic, the other interface is in standby mode.</td>
<td></td>
</tr>
</tbody>
</table>
To disable the MAC address-table move update feature on the access switch, use the `no mac address-table move update transmit` interface configuration command. To display the MAC address-table move update information, use the `show mac address-table move update` privileged EXEC command.

This example shows how to configure an access switch to send MAC address-table move update messages and to verify the configuration:

```
Switch# configure terminal
Switch(config)# interface fastethernet1/0/1
Switch(config-if)# switchport backup interface fastethernet1/0/2 mmu primary vlan 2
Switch(config-if)# end
Switch(config)# mac address-table move update transmit
Switch(config)# end
Switch# show mac-address-table move update
Switch-ID : 01d0.2bfc.3180
Dst mac-address : 0180.c200.0010
Vlans/Macs supported : 1023/8320
Default/Current settings: Rcv Off/Off, Xmt Off/Off
Max packets per min : Rcv 40, Xmt 60
Rcv packet count : 0
Rcv conforming packet count : 0
Rcv invalid packet count : 0
Rcv packet count this min : 0
Rcv threshold exceed count : 0
Rcv last sequence# this min : 0
Rcv last interface : None
Rcv last src-mac-address : 0000.0000.0000
Rcv last switch-ID : 0000.0000.0000
Xmt packet count : 0
Xmt packet count this min : 0
Xmt threshold exceed count : 0
Xmt pak buf unavail cnt : 0
Xmt last interface : None
```

To disable the MAC address-table move update feature on the access switch, use the `no mac address-table move update transmit` interface configuration command. To display the MAC address-table move update information, use the `show mac address-table move update` privileged EXEC command.

This example shows how to configure an access switch to send MAC address-table move update messages and to verify the configuration:

```
Switch# configure terminal
Switch(config)# interface fastethernet1/0/1
Switch(config-if)# switchport backup interface fastethernet1/0/2 mmu primary vlan 2
Switch(config-if)# end
Switch(config)# mac address-table move update transmit
Switch(config)# end
Switch# show mac-address-table move update
Switch-ID : 01d0.2bfc.3180
Dst mac-address : 0180.c200.0010
Vlans/Macs supported : 1023/8320
Default/Current settings: Rcv Off/Off, Xmt Off/Off
Max packets per min : Rcv 40, Xmt 60
Rcv packet count : 0
Rcv conforming packet count : 0
Rcv invalid packet count : 0
Rcv packet count this min : 0
Rcv threshold exceed count : 0
Rcv last sequence# this min : 0
Rcv last interface : None
Rcv last src-mac-address : 0000.0000.0000
Rcv last switch-ID : 0000.0000.0000
Xmt packet count : 0
Xmt packet count this min : 0
Xmt threshold exceed count : 0
Xmt pak buf unavail cnt : 0
Xmt last interface : None
```
Beginning in privileged EXEC mode, follow these steps to configure a switch to get and process MAC address-table move update messages:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 mac address-table move update receive</td>
<td>Enable the switch to get and process the MAC address-table move updates.</td>
</tr>
<tr>
<td>Step 3 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4 show mac address-table move update</td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td>Step 5 copy running-config startup config</td>
<td>(Optional) Save your entries in the switch startup configuration file.</td>
</tr>
</tbody>
</table>

To disable the MAC address-table move update feature on the access switch, use the `no mac address-table move update receive` configuration command. To display the MAC address-table move update information, use the `show mac address-table move update` privileged EXEC command.

This example shows how to configure a switch to get and process MAC address-table move update messages:

Switch# configure terminal
Switch(config)# mac address-table move update receive
Switch(config)# end

### Monitoring Flex Links and the MAC Address-Table Move Update

Table 20-1 shows the privileged EXEC commands for monitoring the Flex Links configuration and the MAC address-table move update information.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show interface [interface-id] switchport backup</td>
<td>Displays the Flex Link backup interface configured for an interface or all the configured Flex Links and the state of each active and backup interface (up or standby mode).</td>
</tr>
<tr>
<td>show mac address-table move update</td>
<td>Displays the MAC address-table move update information on the switch.</td>
</tr>
</tbody>
</table>
CHAPTER 21

Configuring DHCP Features and IP Source Guard

This chapter describes how to configure DHCP snooping and option-82 data insertion, and the DHCP server port-based address allocation features on the Catalyst 3750 Metro switch. It also describes how to configure the IP source guard feature.

Note
For complete syntax and usage information for the commands used in this chapter, see the command reference for this release, and see the “DHCP Commands” section in the Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2.

This chapter consists of these sections:
- Understanding DHCP Features, page 21-1
- Configuring DHCP Features, page 21-8
- Displaying DHCP Snooping Information, page 21-15
- Understanding IP Source Guard, page 21-15
- Configuring IP Source Guard, page 21-17
- Displaying IP Source Guard Information, page 21-25
- Understanding DHCP Server Port-Based Address Allocation, page 21-25
- Configuring DHCP Server Port-Based Address Allocation, page 21-26
- Displaying DHCP Server Port-Based Address Allocation, page 21-29

Understanding DHCP Features

DHCP is widely used in LAN environments to dynamically assign host IP addresses from a centralized server, which significantly reduces the overhead of administration of IP addresses. DHCP also helps conserve the limited IP address space because IP addresses no longer need to be permanently assigned to hosts; only those hosts that are connected to the network consume IP addresses.

The switch supports these DHCP features:
- DHCP Server, page 21-2
- DHCP Relay Agent, page 21-2
- DHCP Snooping, page 21-2
- Option-82 Data Insertion, page 21-3
Understanding DHCP Features

- Cisco IOS DHCP Server Database, page 21-6
- DHCP Snooping Binding Database, page 21-6

For information about the DHCP client, see the “Configuring DHCP” section of the “IP Addressing and Services” section of the Cisco IOS IP Configuration Guide, Release 12.2.

DHCP Server

The DHCP server assigns IP addresses from specified address pools on a switch or router to DHCP clients and manages them. If the DHCP server cannot give the DHCP client the requested configuration parameters from its database, it forwards the request to one or more secondary DHCP servers defined by the network administrator.

DHCP Relay Agent

A DHCP relay agent is a Layer 3 device that forwards DHCP packets between clients and servers. Relay agents forward requests and replies between clients and servers when they are not on the same physical subnet. Relay agent forwarding is different from the normal Layer 2 forwarding, in which IP datagrams are switched transparently between networks. Relay agents receive DHCP messages and generate new DHCP messages to send on egress interfaces.

DHCP Snooping

DHCP snooping is a DHCP security feature that provides network security by filtering untrusted DHCP messages and by building and maintaining a DHCP snooping binding database, also referred to as a DHCP snooping binding table. For more information about this database, see the “Displaying DHCP Snooping Information” section on page 21-15.

DHCP snooping acts like a firewall between untrusted hosts and DHCP servers. You use DHCP snooping to differentiate between untrusted interfaces connected to the end user and trusted interfaces connected to the DHCP server or another switch.

Note

For DHCP snooping to function properly, all DHCP servers must be connected to the switch through trusted interfaces.

An untrusted DHCP message is a message that is received from outside the network or firewall. When you use DHCP snooping in a service-provider environment, an untrusted message is sent from a device that is not in the service-provider network, such as a customer’s switch. Messages from unknown devices are untrusted because they can be sources of traffic attacks.

The DHCP snooping binding database has the MAC address, the IP address, the lease time, the binding type, the VLAN number, and the interface information that corresponds to the local untrusted interfaces of a switch. It does not have information regarding hosts interconnected with a trusted interface.

In a service-provider network, a trusted interface is connected to a port on a device in the same network. An untrusted interface is connected to an untrusted interface in the network or to an interface on a device that is not in the network.
When a switch receives a packet on an untrusted interface and the interface belongs to a VLAN in which DHCP snooping is enabled, the switch compares the source MAC address and the DHCP client hardware address. If the addresses match (the default), the switch forwards the packet. If the addresses do not match, the switch drops the packet.

The switch drops a DHCP packet when one of these situations occurs:

- A packet from a DHCP server, such as a DHCPOFFER, DHCPACK, DHCPNAK, or DHCPLEASEQUERY packet, is received from outside the network or firewall.
- A packet is received on an untrusted interface, and the source MAC address and the DHCP client hardware address do not match.
- The switch receives a DHCPRERELEASE or DHCPDECLINE broadcast message that has a MAC address in the DHCP snooping binding database, but the interface information in the binding database does not match the interface on which the message was received.
- A DHCP relay agent forwards a DHCP packet that includes a relay-agent IP address that is not 0.0.0.0, or the relay agent forwards a packet that includes option-82 information to an untrusted port.

If the switch is an aggregation switch supporting DHCP snooping and is connected to an edge switch that is inserting DHCP option-82 information, the switch drops packets with option-82 information when packets are received on an untrusted interface. If DHCP snooping is enabled and packets are received on a trusted port, the aggregation switch does not learn the DHCP snooping bindings for connected devices and cannot build a complete DHCP snooping binding database.

When option-82 information is inserted by an edge switch in software releases earlier than Cisco IOS Release 12.2(25)EY, you cannot configure DHCP snooping on an aggregation switch because the DHCP snooping bindings database will not be properly populated. You also cannot configure IP source guard and dynamic Address Resolution Protocol (ARP) inspection on the switch unless you use static bindings or ARP access control lists (ACLs).

In Cisco IOS Release 12.2(25)EY or later, when an aggregation switch can be connected to an edge switch through an untrusted interface and you enter the `ip dhcp snooping information option allowed-trust` global configuration command, the aggregation switch accepts packets with option-82 information from the edge switch. The aggregation switch learns the bindings for hosts connected through an untrusted switch interface. The DHCP security features, such as dynamic ARP or IP source guard, can still be enabled on the aggregation switch while the switch receives packets with option-82 information on ingress untrusted interfaces to which hosts are connected. The port on the edge switch that connects to the aggregation switch must be configured as a trusted interface.

### Option-82 Data Insertion

In residential, metropolitan Ethernet-access environments, DHCP can centrally manage the IP address assignments for a large number of subscribers. When the DHCP option-82 feature is enabled on the switch, a subscriber device is identified by the switch port through which it connects to the network (in addition to its MAC address). Multiple hosts on the subscriber LAN can be connected to the same port on the access switch and are uniquely identified.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>The DHCP option-82 feature is supported only when DHCP snooping is enabled globally and on the VLANs to which subscriber devices using this feature are assigned.</td>
</tr>
</tbody>
</table>
Figure 21-1 is an example of a metropolitan Ethernet network in which a centralized DHCP server assigns IP addresses to subscribers connected to the switch at the access layer. Because the DHCP clients and their associated DHCP server do not reside on the same IP network or subnet, a DHCP relay agent (the Catalyst switch) is configured with a helper address to enable broadcast forwarding and to transfer DHCP messages between the clients and the server.

When you enable DHCP snooping information option 82 on the switch, this sequence of events occurs:

- The host (DHCP client) generates a DHCP request and broadcasts it on the network.
- When the switch receives the DHCP request, it adds the option-82 information in the packet. By default, the remote-ID suboption is the switch MAC address, and the circuit-ID suboption is the port identifier, `vlan-mod-port`, from which the packet is received. Beginning with Cisco IOS Release 12.2(25)SEE, you can configure the remote ID and circuit ID. For information on configuring these suboptions, see the “Enabling DHCP Snooping and Option 82” section on page 21-11.
- If the IP address of the relay agent is configured, the switch adds this IP address in the DHCP packet.
- The switch forwards the DHCP request that includes the option-82 field to the DHCP server.
- The DHCP server receives the packet. If the server is option-82-capable, it can use the remote ID, the circuit ID, or both to assign IP addresses and implement policies, such as restricting the number of IP addresses that can be assigned to a single remote ID or circuit ID. Then the DHCP server echoes the option-82 field in the DHCP reply.
- The DHCP server unicasts the reply to the switch if the request was relayed to the server by the switch. The switch verifies that it originally inserted the option-82 data by inspecting the remote-ID and possibly the circuit-ID fields. The switch removes the option-82 field and forwards the packet to the switch port that connects to the DHCP client that sent the DHCP request.

In the default suboption configuration, when the previously described sequence of events occurs, the values in these fields in Figure 21-2 do not change:

- Circuit-ID suboption fields
  - Suboption type
  - Length of the suboption type
  - Circuit-ID type
  - Length of the circuit-ID type
- Remote-ID suboption fields
  - Suboption type
  - Length of the suboption type
  - Remote-ID type
  - Length of the circuit-ID type

In the port field of the circuit-ID suboption, the port numbers start at 3. For example, on the switch, port 3 is the Fast Ethernet 1/0/1 port, port 4 is the Fast Ethernet 1/0/2 port, port 5 is the Fast Ethernet 1/0/3 port, and so on. Port 27 is the small form-factor pluggable (SFP) module slot 1/0/1, and port 28 is the SFP module slot 2/0/2, and so on.

Figure 21-2 shows the packet formats for the default configuration of the remote-ID suboption and the circuit-ID suboption. For the circuit-ID suboption, the module number corresponds to the switch number in the stack. The switch uses the packet formats when DHCP snooping is globally enabled and when the `ip dhcp snooping information option` global configuration command is entered.

**Figure 21-2  Default Suboption Packet Formats**

**Circuit ID Suboption Frame Format**

```
Suboption type | Circuit ID type
-------------|----------------
Length        | Length
1 byte       | 1 byte
```

**Remote ID Suboption Frame Format**

```
Suboption type | Remote ID type
---------------|----------------
Length        | Length
1 byte       | 1 byte
```

Figure 21-3 shows the packet formats for user-configured remote-ID and circuit-ID suboptions. The switch uses these packet formats when you globally enable DHCP snooping and enter the `ip dhcp snooping information option format remote-id` global configuration command and the `ip dhcp snooping vlan information option format-type circuit-id string` interface configuration command.

The values for these fields in the packets change from the default values when you configure the remote-ID and circuit-ID suboptions:
- Circuit-ID suboption fields
  - The circuit-ID type is 1.
  - The length values are variable, depending on the length of the string that you configure.
### Understanding DHCP Features

- Remote-ID suboption fields
  - The remote-ID type is 1.
  - The length values are variable, depending on the length of the string that you configure.

### Cisco IOS DHCP Server Database

During the DHCP-based autoconfiguration process, the designated DHCP server uses the Cisco IOS DHCP server database. It has IP addresses, address bindings, and configuration parameters, such as the boot file.

An address binding is a mapping between an IP address and a MAC address of a host in the Cisco IOS DHCP server database. You can manually assign the client IP address, or the DHCP server can allocate an IP address from a DHCP address pool. For more information about manual and automatic address bindings, see the “Configuring DHCP” chapter of the *Cisco IOS IP Configuration Guide, Release 12.2*.

### DHCP Snooping Binding Database

When DHCP snooping is enabled, the switch uses the DHCP snooping binding database to store information about untrusted interfaces. The database can have up to 8192 bindings.

Each database entry (binding) has an IP address, an associated MAC address, the lease time (in hexadecimal format), the interface to which the binding applies, and the VLAN to which the interface belongs. The database agent stores the bindings in a file at a configured location. At the end of each entry is a checksum that accounts for all the bytes from the start of the file through all the bytes associated with the entry. Each entry is 72 bytes, followed by a space and then the checksum value.
To keep the bindings when the switch reloads, you must use the DHCP snooping database agent. If the agent is disabled, dynamic ARP or IP source guard is enabled, and the DHCP snooping binding database has dynamic bindings, the switch loses its connectivity. If the agent is disabled and only DHCP snooping is enabled, the switch does not lose its connectivity, but DHCP snooping might not prevent DHCP spoofing attacks.

When reloading, the switch reads the binding file to build the DHCP snooping binding database. The switch updates the file when the database changes.

When a switch learns of new bindings or when it loses bindings, the switch immediately updates the entries in the database. The switch also updates the entries in the binding file. The frequency at which the file is updated is based on a configurable delay, and the updates are batched. If the file is not updated in a specified time (set by the write-delay and abort-timeout values), the update stops.

This is the format of the file that has the bindings:

```
<initial-checksum>
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
<entry-1> <checksum-1>
<entry-2> <checksum-1-2>
...  
<entry-n> <checksum-1-2-..-n>
END
```

Each entry in the file is tagged with a checksum value that the switch uses to verify the entries when it reads the file. The `initial-checksum` entry on the first line distinguishes entries associated with the latest file update from entries associated with a previous file update.

This is an example of a binding file:

```
2bb4c2a1
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
 192.1.168.1 3 0003.47d8.c91f 2BB6488E Fa1/0/4 21ae5fbb
 192.1.168.3 3 0003.44d6.c52f 2BB648EB Fa1/0/4 1bdb223f
 192.1.168.2 3 0003.47d9.c8f1 2BB648AB Fa1/0/4 584a38f0
END
```

When the switch starts and the calculated checksum value equals the stored checksum value, the switch reads entries from the binding file and adds the bindings to its DHCP snooping binding database. The switch ignores an entry when one of these situations occurs:

- The switch reads the entry and the calculated checksum value does not equal the stored checksum value. The entry and the ones following it are ignored.
- An entry has an expired lease time (the switch might not remove a binding entry when the lease time expires).
- The interface in the entry no longer exists on the system.
- The interface is a routed interface or a DHCP snooping-trusted interface.
Configuring DHCP Features

These sections describe how to configure the DHCP server, the DHCP relay agent, DHCP snooping, and option 82, the Cisco IOS DHCP server binding database, and the DHCP snooping binding database on your switch:

- Default DHCP Configuration, page 21-8
- DHCP Snooping Configuration Guidelines, page 21-9
- Configuring the DHCP Server, page 21-10
- Configuring the DHCP Relay Agent, page 21-10
- Specifying the Packet Forwarding Address, page 21-10
- Enabling DHCP Snooping and Option 82, page 21-11
- Enabling DHCP Snooping on Private VLANs, page 21-13
- Enabling the Cisco IOS DHCP Server Database, page 21-14
- Enabling the DHCP Snooping Binding Database Agent, page 21-14

Default DHCP Configuration

Table 21-1 shows the default DHCP configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP server</td>
<td>Enabled&lt;sup&gt;1&lt;/sup&gt;</td>
</tr>
<tr>
<td>DHCP relay agent</td>
<td>Enabled&lt;sup&gt;2&lt;/sup&gt;</td>
</tr>
<tr>
<td>DHCP packet forwarding address</td>
<td>None configured</td>
</tr>
<tr>
<td>Checking the relay agent information</td>
<td>Enabled (invalid messages are dropped)&lt;sup&gt;2&lt;/sup&gt;</td>
</tr>
<tr>
<td>DHCP relay agent forwarding policy</td>
<td>Replace the existing relay agent information&lt;sup&gt;3&lt;/sup&gt;</td>
</tr>
<tr>
<td>Cisco IOS DHCP server binding database</td>
<td>Enabled&lt;sup&gt;1&lt;/sup&gt;</td>
</tr>
<tr>
<td>DHCP snooping enabled globally</td>
<td>Disabled</td>
</tr>
<tr>
<td>DHCP snooping information option</td>
<td>Enabled</td>
</tr>
<tr>
<td>DHCP snooping option to accept packets on untrusted ingress interfaces&lt;sup&gt;4&lt;/sup&gt;</td>
<td>Disabled</td>
</tr>
<tr>
<td>DHCP snooping limit rate</td>
<td>None configured</td>
</tr>
<tr>
<td>DHCP snooping trust</td>
<td>Untrusted</td>
</tr>
<tr>
<td>DHCP snooping VLAN</td>
<td>Disabled</td>
</tr>
<tr>
<td>DHCP snooping MAC address verification</td>
<td>Enabled</td>
</tr>
<tr>
<td>DHCP snooping binding database agent&lt;sup&gt;1&lt;/sup&gt;</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

1. The switch responds to DHCP requests only if it is configured as a DHCP server.
2. The switch relays DHCP packets only if the IP address of the DHCP server is configured on the SVI of the DHCP client.
3. The switch gets network addresses and configuration parameters only from a device configured as DHCP server.
4. Use this feature when the switch is an aggregation switch that receives packets with option-82 information from an edge switch.
DHCP Snooping Configuration Guidelines

These are the configuration guidelines for DHCP snooping.

- You must globally enable DHCP snooping on the switch.
- DHCP snooping is not active until DHCP snooping is enabled on a VLAN.
- Before globally enabling DHCP snooping on the switch, make sure that the devices acting as the DHCP server and the DHCP relay agent are configured and enabled.
- Before configuring the DHCP snooping information option on your switch, be sure to configure the device that is acting as the DHCP server. For example, you must specify the IP addresses that the DHCP server can assign or exclude, or you must configure DHCP options for these devices.

**Note**

Do not enable Dynamic Host Configuration Protocol (DHCP) snooping on RSPAN VLANs. If DHCP snooping is enabled on RSPAN VLANs, DHCP packets might not reach the RSPAN destination port.

- When configuring a large number of circuit IDs on a switch, consider the impact of lengthy character strings on the NVRAM or the flash memory. If the circuit-ID configurations, combined with other data, exceed the capacity of the NVRAM or the flash memory, an error message appears.
- Before configuring the DHCP relay agent on your switch, make sure to configure the device that is acting as the DHCP server. For example, you must specify the IP addresses that the DHCP server can assign or exclude, configure DHCP options for devices, or set up the DHCP database agent.
- If the DHCP relay agent is enabled but DHCP snooping is disabled, the DHCP option-82 data insertion feature is not supported.
- If a switch port is connected to a DHCP server, configure a port as trusted by entering the `ip dhcp snooping trust` interface configuration command.
- If a switch port is connected to a DHCP client, configure a port as untrusted by entering the `no ip dhcp snooping trust` interface configuration command.
- Follow these guidelines when configuring the DHCP snooping binding database:
  - Because both NVRAM and the flash memory have limited storage capacity, we recommend that you store the binding file on a TFTP server.
  - For network-based URLs (such as TFTP and FTP), you must create an empty file at the configured URL before the switch can write bindings to the binding file at that URL. See the documentation for your TFTP server to determine whether you must first create an empty file on the server; some TFTP servers cannot be configured this way.
  - To ensure that the lease time in the database is accurate, we recommend that you enable and configure NTP. For more information, see the “Configuring NTP” section on page 5-3.
  - If NTP is configured, the switch writes binding changes to the binding file only when the switch system clock is synchronized with NTP.
- Do not enter the `ip dhcp snooping information option allowed-untrusted` command on an aggregation switch to which an untrusted device is connected. If you enter this command, an untrusted device might spoof the option-82 information.
- Starting with Cisco IOS Release 12.2(37)SE, you can display DHCP snooping statistics by entering the `show ip dhcp snooping statistics` user EXEC command, and you can clear the snooping statistics counters by entering the `clear ip dhcp snooping statistics` privileged EXEC command.
Configuring DHCP Features

Note
Do not enable Dynamic Host Configuration Protocol (DHCP) snooping on RSPAN VLANs. If DHCP snooping is enabled on RSPAN VLANs, DHCP packets might not reach the RSPAN destination port.

Chapter 21      Configuring DHCP Features and IP Source Guard

Configuring DHCP Features

Note
Do not enable Dynamic Host Configuration Protocol (DHCP) snooping on RSPAN VLANs. If DHCP snooping is enabled on RSPAN VLANs, DHCP packets might not reach the RSPAN destination port.

Configuring the DHCP Server

The switch can act as a DHCP server. By default, the Cisco IOS DHCP server and relay agent features are enabled on your switch but are not configured. These features are not operational.

For procedures to configure the switch as a DHCP server, see the “Configuring DHCP” section of the “IP addressing and Services” section of the Cisco IOS IP Configuration Guide, Release 12.2.

Configuring the DHCP Relay Agent

Beginning in privileged EXEC mode, follow these steps to enable the DHCP relay agent on the switch:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>service dhcp</td>
<td>Enable the DHCP server and relay agent on your switch. By default, this feature is enabled.</td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable the DHCP server and relay agent, use the no service dhcp global configuration command.

See the “Configuring DHCP” section of the “IP Addressing and Services” section of the Cisco IOS IP Configuration Guide, Release 12.2 for these procedures:

- Checking (validating) the relay agent information
- Configuring the relay agent forwarding policy

Specifying the Packet Forwarding Address

If the DHCP server and the DHCP clients are on different networks or subnets, you must configure the switch with the ip helper-address address interface configuration command. The general rule is to configure the command on the Layer 3 interface closest to the client. The address used in the ip helper-address command can be a specific DHCP server IP address, or it can be the network address if other DHCP servers are on the destination network segment. Using the network address enables any DHCP server to respond to requests.
Beginning in privileged EXEC mode, follow these steps to specify the packet forwarding address:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> interface vlan vlan-id</td>
<td>Enter interface configuration mode, and create a switch virtual interface.</td>
</tr>
<tr>
<td><strong>Step 3</strong> ip address ip-address subnet-mask</td>
<td>Configure the interface with an IP address and an IP subnet.</td>
</tr>
<tr>
<td><strong>Step 4</strong> ip helper-address address</td>
<td>Specify the DHCP packet forwarding address. The helper address can be a specific DHCP server address, or it can be the network address if other DHCP servers are on the destination network segment. Using the network address enables other servers to respond to DHCP requests. If you have multiple servers, you can configure one helper address for each server.</td>
</tr>
<tr>
<td><strong>Step 5</strong> exit</td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 6</strong> interface range port-range</td>
<td>Configure multiple physical ports that are connected to the DHCP clients, and enter interface range configuration mode.</td>
</tr>
<tr>
<td><strong>Step 7</strong> switchport mode access</td>
<td>Define the VLAN membership mode for the port.</td>
</tr>
<tr>
<td><strong>Step 8</strong> switchport access vlan vlan-id</td>
<td>Assign the ports to the same VLAN as configured in Step 2.</td>
</tr>
<tr>
<td><strong>Step 9</strong> end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 10</strong> show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td><strong>Step 11</strong> copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To remove the DHCP packet forwarding address, use the `no ip helper-address address` interface configuration command.

### Enabling DHCP Snooping and Option 82

Beginning in privileged EXEC mode, follow these steps to enable DHCP snooping on the switch:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> ip dhcp snooping</td>
<td>Enable DHCP snooping globally.</td>
</tr>
</tbody>
</table>
## Configuring DHCP Features

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>ip dhcp snooping vlan vlan-range</strong>&lt;br&gt;Enable DHCP snooping on a VLAN or range of VLANs. The range is 1 to 4094. You can enter a single VLAN ID identified by VLAN ID number, a series of VLAN IDs separated by commas, a range of VLAN IDs separated by hyphens, or a range of VLAN IDs separated by entering the starting and ending VLAN IDs separated by a space.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>ip dhcp snooping information option</strong>&lt;br&gt;Enable the switch to insert and remove DHCP relay information (option-82 field) in forwarded DHCP request messages to the DHCP server. The default is enabled.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>**ip dhcp snooping information option format remote-id [string ASCII-string</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>ip dhcp snooping information option allowed-untrusted</strong>&lt;br&gt;(Optional) If the switch is an aggregation switch connected to an edge switch, enable the switch to accept incoming DHCP snooping packets with option-82 information from the edge switch. The default is disabled.&lt;br&gt;Note You must only enter this command on aggregation switches that are connected to trusted devices.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>interface interface-id</strong>&lt;br&gt;Enter interface configuration mode, and specify the interface to be configured.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><strong>ip dhcp snooping vlan vlan information option format-type circuit-id [override] string ASCII-string</strong>&lt;br&gt;(Optional) Configure the circuit-ID suboption for the specified interface. Specify the VLAN and port identifier, using a VLAN ID in the range of 1 to 4094. The default circuit ID is the port identifier, in the format <code>vlan-mod-port</code>. You can configure the circuit ID to be a string of 3 to 63 ASCII characters (no spaces).&lt;br&gt;(Optional) Use the <code>override</code> keyword when you do not want the circuit-ID suboption inserted in TLV format to define subscriber information.</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td><strong>ip dhcp snooping trust</strong>&lt;br&gt;(Optional) Configure the interface as trusted or untrusted. You can use the <code>no</code> keyword to configure an interface to receive messages from an untrusted client. The default is untrusted.</td>
</tr>
</tbody>
</table>
Chapter 21  Configuring DHCP Features and IP Source Guard

Configuring DHCP Features

To disable DHCP snooping, use the `no ip dhcp snooping` global configuration command. To disable DHCP snooping on a VLAN or range of VLANs, use the `no ip dhcp snooping vlan vlan-range` global configuration command. To disable the insertion and removal of the option-82 field, use the `no ip dhcp snooping information option` global configuration command. To configure an aggregation switch to drop incoming DHCP snooping packets with option-82 information from an edge switch, use the `no ip dhcp snooping information option allowed-untrusted` global configuration command.

This example shows how to enable DHCP snooping globally and on VLAN 10 and to configure a rate limit of 100 packets per second on a port:

```
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10
Switch(config)# ip dhcp snooping information option
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip dhcp snooping limit rate 100
```

Enabling DHCP Snooping on Private VLANs

You can enable DHCP snooping on private VLANs. If DHCP snooping is enabled, the configuration is propagated to both a primary VLAN and its associated secondary VLANs. If DHCP snooping is enabled on the primary VLAN, it is also configured on the secondary VLANs.

If DHCP snooping is already configured on the primary VLAN and you configure DHCP snooping with different settings on a secondary VLAN, the configuration for the secondary VLAN does not take effect. You must configure DHCP snooping on the primary VLAN. If DHCP snooping is not configured on the primary VLAN, this message appears when you are configuring DHCP snooping on the secondary VLAN, such as VLAN 200:

```
2w5d:%DHCP_SNOOPING-4-DHCP_SNOOPING_PVLAN_WARNING:DHCP Snooping configuration may not take effect on secondary vlan 200. DHCP Snooping configuration on secondary vlan is derived from its primary vlan.
```

The `show ip dhcp snooping` privileged EXEC command output shows all VLANs, including primary and secondary private VLANs, on which DHCP snooping is enabled.
Enabling the Cisco IOS DHCP Server Database

For procedures to enable and configure the Cisco IOS DHCP server database, see the “DHCP Configuration Task List” section in the “Configuring DHCP” chapter of the Cisco IOS IP Configuration Guide, Release 12.2.

Enabling the DHCP Snooping Binding Database Agent

Beginning in privileged EXEC mode, follow these steps to enable and configure the DHCP snooping binding database agent on the switch.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip dhcp snooping database {flash://filename</td>
</tr>
<tr>
<td></td>
<td>ftp://username:password@host//filename</td>
</tr>
<tr>
<td></td>
<td>http://[username:password@] [hostname</td>
</tr>
<tr>
<td></td>
<td>\host-ip]/[directory</td>
</tr>
<tr>
<td></td>
<td>image-name.tar</td>
</tr>
<tr>
<td></td>
<td>rcp://username@host//filename</td>
</tr>
<tr>
<td></td>
<td>tftp://host//filename</td>
</tr>
<tr>
<td>Step 3</td>
<td>ip dhcp snooping database timeout seconds</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>ip dhcp snooping database write-delay seconds</td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
</tr>
<tr>
<td>Step 6</td>
<td>ip dhcp snooping binding mac-address vlan vlan-id ip-address interface interface-id expiry seconds</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td>show ip dhcp snooping database [detail]</td>
</tr>
<tr>
<td>Step 8</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To stop using the database agent and binding files, use the **no ip dhcp snooping database** global configuration command. To reset the timeout or delay values, use the **ip dhcp snooping database timeout seconds** or the **ip dhcp snooping database write-delay seconds** global configuration command.
To clear the statistics of the DHCP snooping binding database agent, use the `clear ip dhcp snooping
database statistics` privileged EXEC command. To renew the database, use the `renew ip dhcp snooping
database` privileged EXEC command.

To delete binding entries from the DHCP snooping binding database, use the `no ip dhcp snooping
binding mac-address vlan vlan-id ip-address interface interface-id` privileged EXEC command. Enter
this command for each entry that you want to delete.

**Displaying DHCP Snooping Information**

To display the DHCP snooping information, use the privileged EXEC commands in Table 21-2:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip dhcp snooping</td>
<td>Displays the DHCP snooping configuration for a switch</td>
</tr>
<tr>
<td>show ip dhcp snooping binding</td>
<td>Displays only the dynamically configured bindings in the DHCP snooping binding database, also referred to as a binding table.¹</td>
</tr>
<tr>
<td>show ip dhcp snooping database</td>
<td>Displays the DHCP snooping binding database status and statistics.</td>
</tr>
<tr>
<td>show ip dhcp snooping statistics</td>
<td>Displays the DHCP snooping statistics in summary or detail form.</td>
</tr>
<tr>
<td>show ip source binding</td>
<td>Display the dynamically and statically configured bindings.</td>
</tr>
</tbody>
</table>

¹. If DHCP snooping is enabled and an interface changes to the down state, the switch does not delete the manually configured bindings.

**Note**

If DHCP snooping is enabled and an interface changes to the down state, the switch does not delete the statically configured bindings.

**Understanding IP Source Guard**

IPSG is a security feature that restricts IP traffic on nonrouted, Layer 2 interfaces by filtering traffic based on the DHCP snooping binding database and on manually configured IP source bindings. You can use IP source guard to prevent traffic attacks if a host tries to use the IP address of its neighbor.

You can enable IP source guard when DHCP snooping is enabled on an untrusted interface. After IPSG is enabled on an interface, the switch blocks all IP traffic received on the interface except for DHCP packets allowed by DHCP snooping. A port access control list (ACL) is applied to the interface. The port ACL allows only IP traffic with a source IP address in the IP source binding table and denies all other traffic.

**Note**

The port ACL takes precedence over any router ACLs or VLAN maps that affect the same interface.
The IP source binding table bindings are learned by DHCP snooping or are manually configured (static IP source bindings). An entry in this table has an IP address with its associated MAC address and VLAN number. The switch uses the IP source binding table only when IP source guard is enabled.

IPSG is supported only on Layer 2 ports, including access and trunk ports. You can configure IPSG with source IP address filtering or with source IP and MAC address filtering.

- Source IP Address Filtering, page 21-16
- Source IP and MAC Address Filtering, page 21-16
- IP Source Guard for Static Hosts, page 21-16

### Source IP Address Filtering

When IPSG is enabled with this option, IP traffic is filtered based on the source IP address. The switch forwards IP traffic when the source IP address matches an entry in the DHCP snooping binding database or a binding in the IP source binding table.

When a DHCP snooping binding or static IP source binding is added, changed, or deleted on an interface, the switch modifies the port ACL using the IP source binding changes, and re-applies the port ACL to the interface.

If you enable IP source guard on an interface on which IP source bindings (dynamically learned by DHCP snooping or manually configured) are not configured, the switch creates and applies a port ACL that denies all IP traffic on the interface. If you disable IP source guard, the switch removes the port ACL from the interface.

### Source IP and MAC Address Filtering

IP traffic is filtered based on the source IP and MAC addresses. The switch forwards traffic only when the source IP and MAC addresses match an entry in the IP source binding table.

When address filtering is enabled, the switch filters IP and non-IP traffic. If the source MAC address of an IP or non-IP packet matches a valid IP source binding, the switch forwards the packet. The switch drops all other types of packets except DHCP packets.

The switch uses port security to filter source MAC addresses. The interface can shut down when a port-security violation occurs.

### IP Source Guard for Static Hosts

**Note**

Do not use IPSG for static hosts on uplink ports or trunk ports.

IPSG for static hosts extends the IPSG capability to non-DHCP and static environments. The previous IPSG used the entries created by DHCP snooping to validate the hosts connected to a switch. Any traffic received from a host without a valid DHCP binding entry is dropped. This security feature restricts IP traffic on nonrouted Layer 2 interfaces. It filters traffic based on the DHCP snooping binding database and on manually configured IP source bindings. The previous version of IPSG required a DHCP environment for IPSG to work.
IPSG for static hosts allows IPSG to work without DHCP. IPSG for static hosts relies on IP device tracking-table entries to install port ACLs. The switch creates static entries based on ARP requests or other IP packets to maintain the list of valid hosts for a given port. You can also specify the number of hosts allowed to send traffic to a given port. This is equivalent to port security at Layer 3.

IPSG for static hosts also supports dynamic hosts. If a dynamic host receives a DHCP-assigned IP address that is available in the IP DHCP snooping table, the same entry is learned by the IP device tracking table. When you enter the `show ip device tracking all` EXEC command, the IP device tracking table displays the entries as ACTIVE.

**Note**

Some IP hosts with multiple network interfaces can inject some invalid packets into a network interface. The invalid packets contain the IP or MAC address for another network interface of the host as the source address. The invalid packets can cause IPSG for static hosts to connect to the host, to learn the invalid IP or MAC address bindings, and to reject the valid bindings. Consult the vendor of the corresponding operating system and the network interface to prevent the host from injecting invalid packets.

IPSG for static hosts initially learns IP or MAC bindings dynamically through an ACL-based snooping mechanism. IP or MAC bindings are learned from static hosts by ARP and IP packets. They are stored in the device tracking database. When the number of IP addresses that have been dynamically learned or statically configured on a given port reaches a maximum, the hardware drops any packet with a new IP address. To resolve hosts that have moved or gone away for any reason, IPSG for static hosts leverages IP device tracking to age out dynamically learned IP address bindings. This feature can be used with DHCP snooping. Multiple bindings are established on a port that is connected to both DHCP and static hosts. For example, bindings are stored in both the device tracking database as well as in the DHCP snooping binding database.

### Configuring IP Source Guard

- **Default IP Source Guard Configuration**, page 21-17
- **IP Source Guard Configuration Guidelines**, page 21-17
- **Enabling IP Source Guard**, page 21-18
- **Configuring IP Source Guard for Static Hosts**, page 21-19

### Default IP Source Guard Configuration

By default, IP source guard is disabled.

### IP Source Guard Configuration Guidelines

- You can configure static IP bindings only on nonrouted ports. If you enter the `ip source binding mac-address vlan vlan-id ip-address interface interface-id` global configuration command on a routed interface, this error message appears:

  Static IP source binding can only be configured on switch port.

- When IP source guard with source IP filtering is enabled on an interface, DHCP snooping must be enabled on the access VLAN for that interface.
If you are enabling IP source guard on a trunk interface with multiple VLANs and DHCP snooping is enabled on all the VLANs, the source IP address filter is applied on all the VLANs.

**Note** If IP source guard is enabled and you enable or disable DHCP snooping on a VLAN on the trunk interface, the switch might not properly filter traffic.

- If you enable IP source guard with source IP and MAC address filtering, DHCP snooping and port security must be enabled on the interface. You must also enter the `ip dhcp snooping information option` global configuration command and ensure that the DHCP server supports option 82. When IP source guard is enabled with MAC address filtering, the DHCP host MAC address is not learned until the host is granted a lease. When forwarding packets from the server to the host, DHCP snooping uses option-82 data to identify the host port.

- When configuring IP source guard on interfaces on which a private VLAN is configured, port security is not supported.

- IP source guard is not supported on EtherChannels.

- You can enable this feature when IEEE 802.1x port-based authentication is enabled.

- If the number of ternary content addressable memory (TCAM) entries exceeds the maximum available, the CPU usage increases.

## Enabling IP Source Guard

Beginning in privileged EXEC mode, follow these steps to enable and configure IP source guard on an interface.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: <code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2: <code>interface interface-id</code></td>
<td>Enter interface configuration mode, and specify the interface to be configured.</td>
</tr>
<tr>
<td>Step 3: <code>ip verify source</code></td>
<td>Enable IP source guard with source IP address filtering.</td>
</tr>
<tr>
<td>or <code>ip verify source port-security</code></td>
<td>Enable IP source guard with source IP and MAC address filtering.</td>
</tr>
<tr>
<td>Note</td>
<td>When you enable both IP source guard and port security, using the <code>ip verify source port-security</code> interface configuration command, there are two caveats:</td>
</tr>
<tr>
<td></td>
<td>- The DHCP server must support option 82, or the client is not assigned an IP address.</td>
</tr>
<tr>
<td></td>
<td>- The MAC address in the DHCP packet is not learned as a secure address. The MAC address of the DHCP client is learned as a secure address only when the switch receives non-DHCP data traffic.</td>
</tr>
<tr>
<td>Step 4: <code>exit</code></td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td>Step 5: <code>ip source binding mac-address vlan vlan-id ip-address interface interface-id</code></td>
<td>Add a static IP source binding. Enter this command for each static binding.</td>
</tr>
</tbody>
</table>
Configuring IP Source Guard for Static Hosts

- Configuring IP Source Guard for Static Hosts on a Layer 2 Access Port, page 21-19
- Configuring IP Source Guard for Static Hosts on a Private VLAN Host Port, page 21-23

**Configuring IP Source Guard for Static Hosts on a Layer 2 Access Port**

**Note**  
You must configure the `ip device tracking maximum limit-number` interface configuration command globally for IPSG for static hosts to work. If you only configure this command on a port without enabling IP device tracking globally or by setting an IP device tracking maximum on that interface, IPSG with static hosts rejects all the IP traffic from that interface. This requirement also applies to IPSG with static hosts on a private VLAN host port.

Beginning in privileged EXEC mode:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>ip device tracking</td>
<td>Turn on the IP host table, and globally enable IP device tracking.</td>
</tr>
<tr>
<td>3</td>
<td>interface interface-id</td>
<td>Enter interface configuration mode.</td>
</tr>
</tbody>
</table>

To disable IP source guard with source IP address filtering, use the `no ip verify source` interface configuration command.

To delete a static IP source binding entry, use the `no ip source global` configuration command.

This example shows how to enable IP source guard with source IP and MAC filtering on VLANs 10 and 11:

Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip verify source port-security
Switch(config-if)# exit
Switch(config)# ip source binding 0100.0022.0010 vlan 10 10.0.0.2 interface gigabitethernet1/0/1
Switch(config)# ip source binding 0100.0230.0002 vlan 11 10.0.0.4 interface gigabitethernet1/0/1
Switch(config)# end

To disable IP source guard with source IP address filtering, use the `no ip verify source` interface configuration command.

To delete a static IP source binding entry, use the `no ip source global` configuration command.

This example shows how to enable IP source guard with source IP and MAC filtering on VLANs 10 and 11:

Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip verify source port-security
Switch(config-if)# exit
Switch(config)# ip source binding 0100.0022.0010 vlan 10 10.0.0.2 interface gigabitethernet1/0/1
Switch(config)# ip source binding 0100.0230.0002 vlan 11 10.0.0.4 interface gigabitethernet1/0/1
Switch(config)# end
Configuring IP Source Guard

This example shows how to stop IPSG with static hosts on an interface.

```
Switch(config-if)# no ip verify source
Switch(config-if)# no ip device tracking max
```

This example shows how to enable IPSG with static hosts on a port.

```
Switch(config)# ip device tracking
Switch(config)# ip device tracking max 10
Switch(config-if)# ip verify source tracking port-security
```

This example shows how to enable IPSG for static hosts with IP filters on a Layer 2 access port and to verify the valid IP bindings on the interface Gi1/0/3:

```
Step 4
switchport mode access
Configure a port as access.

Step 5
switchport access vlan vlan-id
Configure the VLAN for this port.

Step 6
ip verify source tracking port-security
Enable IPSG for static hosts with MAC address filtering.

Note When you enable both IP source guard and port security by using the `ip verify source port-security` interface configuration command:

- The DHCP server must support option 82, or the client is not assigned an IP address.
- The MAC address in the DHCP packet is not learned as a secure address. The MAC address of the DHCP client is learned as a secure address only when the switch receives non-DHCP data traffic.

Step 7
ip device tracking maximum number
Establish a maximum limit for the number of static IPs that the IP device tracking table allows on the port. The range is 1 to 10. The maximum number is 10.

Note You must configure the `ip device tracking maximum limit-number` interface configuration command.

Step 8
switchport port-security
(Optional) Activate port security for this port.

Step 9
switchport port-security maximum value
(Optional) Establish a maximum of MAC addresses for this port.

Step 10
end
Return to privileged EXEC mode.

Step 11
show ip verify source interface interface-id
Verify the configuration and display IPSG permit ACLs for static hosts.

Step 12
show ip device track all [active | inactive] count
Verify the configuration by displaying the IP-to-MAC binding for a given host on the switch interface.

- `all active`—display only the active IP or MAC binding entries
- `all inactive`—display only the inactive IP or MAC binding entries
- `all`—display the active and inactive IP or MAC binding entries
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip device tracking
Switch(config)# interface gigabitethernet1/0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# ip device tracking maximum 5
Switch(config-if)# ip verify source tracking
Switch(config-if)# end

Switch# show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----
Gi1/0/3    ip trk      active       40.1.1.24                           10
Gi1/0/3    ip trk      active       40.1.1.20                           10
Gi1/0/3    ip trk      active       40.1.1.21                           10

This example shows how to enable IPSG for static hosts with IP-MAC filters on a Layer 2 access port, to verify the valid IP-MAC bindings on the interface Gi1/0/3, and to verify that the number of bindings on this interface has reached the maximum:

Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip device tracking
Switch(config)# interface gigabitethernet1/0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 1
Switch(config-if)# ip device tracking maximum 5
Switch(config-if)# switchport port-security
Switch(config-if)# ip verify source tracking port-security
Switch(config-if)# end

Switch# show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----
Gi1/0/3    ip-mac trk   active       40.1.1.24        00:00:00:00:03:04  1
Gi1/0/3    ip-mac trk   active       40.1.1.20        00:00:00:00:03:05  1
Gi1/0/3    ip-mac trk   active       40.1.1.21        00:00:00:00:03:06  1
Gi1/0/3    ip-mac trk   active       40.1.1.22        00:00:00:00:03:07  1
Gi1/0/3    ip-mac trk   active       40.1.1.23        00:00:00:00:03:08  1

This example displays all IP or MAC binding entries for all interfaces. The CLI displays all active as well as inactive entries. When a host is learned on an interface, the new entry is marked as active. When the same host is disconnected from that interface and connected to a different interface, a new IP or MAC binding entry displays as active as soon as the host is detected. The old entry for this host on the previous interface is marked as INACTIVE.

Switch# show ip device tracking all
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
---------------------------------------------------------------------
IP Address     MAC Address   Vlan  Interface              STATE
---------------------------------------------------------------------
200.1.1.8       0001.0600.0000  8    GigabitEthernet1/0/1     INACTIVE
200.1.1.9       0001.0600.0000  8    GigabitEthernet1/0/1     INACTIVE
200.1.1.10      0001.0600.0000  8    GigabitEthernet1/0/1     INACTIVE
200.1.1.11      0001.0600.0000  9    GigabitEthernet1/0/2     ACTIVE
200.1.1.12      0001.0600.0000  9    GigabitEthernet1/0/2     ACTIVE
200.1.1.13      0001.0600.0000  9    GigabitEthernet1/0/2     ACTIVE
This example displays all active IP or MAC binding entries for all interfaces:

Switch# show ip device tracking all active
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30

<table>
<thead>
<tr>
<th>IP Address</th>
<th>MAC Address</th>
<th>Vlan</th>
<th>Interface</th>
<th>STATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>200.1.1.1</td>
<td>0001.0600.0000</td>
<td>9</td>
<td>GigabitEthernet1/0/1</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>200.1.1.2</td>
<td>0001.0600.0000</td>
<td>9</td>
<td>GigabitEthernet1/0/1</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>200.1.1.3</td>
<td>0001.0600.0000</td>
<td>9</td>
<td>GigabitEthernet1/0/1</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>200.1.1.4</td>
<td>0001.0600.0000</td>
<td>9</td>
<td>GigabitEthernet1/0/1</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>200.1.1.5</td>
<td>0001.0600.0000</td>
<td>9</td>
<td>GigabitEthernet1/0/1</td>
<td>ACTIVE</td>
</tr>
</tbody>
</table>

Note that the state of some interfaces is INACTIVE, indicating that they are not actively tracking the IP addresses.
Configuring IP Source Guard

**Configuring IP Source Guard for Static Hosts on a Private VLAN Host Port**

**Note**

You must globally configure the `ip device tracking maximum limit-number` interface configuration command globally for IPSG for static hosts to work. If you only configure this command on a port without enabling IP device tracking globally or setting an IP device tracking maximum on that interface, IPSG with static hosts will reject all the IP traffic from that interface. This requirement also applies to IPSG with static hosts on a Layer 2 access port.

Beginning in privileged EXEC mode, follow these steps to configure IPSG for static hosts with IP filters on a Layer 2 access port:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>vlan vlan-id1</td>
<td>Enter VLAN configuration mode.</td>
</tr>
<tr>
<td>3</td>
<td>private-vlan primary</td>
<td>Establish a primary VLAN on a private VLAN port.</td>
</tr>
<tr>
<td>4</td>
<td>exit</td>
<td>Exit VLAN configuration mode.</td>
</tr>
<tr>
<td>5</td>
<td>vlan vlan-id2</td>
<td>Enter configuration VLAN mode for another VLAN.</td>
</tr>
<tr>
<td>6</td>
<td>private-vlan isolated</td>
<td>Establish an isolated VLAN on a private VLAN port.</td>
</tr>
<tr>
<td>7</td>
<td>exit</td>
<td>Exit VLAN configuration mode.</td>
</tr>
<tr>
<td>8</td>
<td>vlan vlan-id1</td>
<td>Enter configuration VLAN mode.</td>
</tr>
<tr>
<td>9</td>
<td>private-vlan association 201</td>
<td>Associate the VLAN on an isolated private VLAN port.</td>
</tr>
</tbody>
</table>
This example shows how to enable IPSG for static hosts with IP filters on a private VLAN host port:

```
Switch(config)# vlan 200
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# exit
Switch(config)# vlan 201
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# exit
Switch(config)# vlan 200
Switch(config-vlan)# private-vlan association 201
Switch(config-vlan)# exit
Switch(config)# int gigabitethernet1/0/3
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 200 201
Switch(config-if)# ip device tracking maximum 8
Switch(config-if)# ip verify source tracking
```

```
Switch# show ip device tracking all
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30

+----------------+----------------+------------+----------+--------+
| IP Address     | MAC Address    | Vlan       | Interface| State  |
+----------------+----------------+------------+----------+--------+
| 40.1.1.24      | 0000.0000.0304 | 200        | FastEthernet0/3 | ACTIVE |
| 40.1.1.20      | 0000.0000.0305 | 200        | FastEthernet0/3 | ACTIVE |
| 40.1.1.21      | 0000.0000.0306 | 200        | FastEthernet0/3 | ACTIVE |
| 40.1.1.22      | 0000.0000.0307 | 200        | FastEthernet0/3 | ACTIVE |
| 40.1.1.23      | 0000.0000.0308 | 200        | FastEthernet0/3 | ACTIVE |
```

---

**Command** | **Purpose**
--- | ---
Step 10 | exit
Step 11 | interface fastEthernet *interface-id*
Step 12 | switchport mode private-vlan host
Step 13 | switchport private-vlan host-association *vlan-id1* *
Step 14 | ip device tracking maximum *number*
Step 15 | ip verify source tracking [port-security]
Step 16 | end
Step 17 | show ip device tracking all
Step 18 | show ip verify source interface *interface-id*

**Note**

You must globally configure the `ip device tracking maximum number` interface command for IPSG for static hosts to work.

**Step 10**

Exit VLAN configuration mode.

**Step 11**

Enter interface configuration mode.

**Step 12**

(Optional) Establish a port as a private VLAN host.

**Step 13**

(Optional) Associate this port with the corresponding private VLAN.

**Step 14**

Establish a maximum for the number of static IPs that the IP device tracking table allows on the port.

The maximum is 10.

**Step 15**

Activate IPSG for static hosts with MAC address filtering on this port.

**Step 16**

Exit configuration interface mode.

**Step 17**

Verify the configuration.

**Step 18**

Verify the IP source guard configuration. Display IPSG permit ACLs for static hosts.
The output shows the five valid IP-MAC bindings that have been learned on the interface Gi1/0/3. For the private VLAN cases, the bindings are associated with primary VLAN ID. So, in this example, the primary VLAN ID, 200, is shown in the table.

<table>
<thead>
<tr>
<th>Interface</th>
<th>Filter-type</th>
<th>Filter-mode</th>
<th>IP-address</th>
<th>Mac-address</th>
<th>Vlan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/3</td>
<td>ip trk</td>
<td>active</td>
<td>40.1.1.23</td>
<td></td>
<td>200</td>
</tr>
<tr>
<td>Gi1/0/3</td>
<td>ip trk</td>
<td>active</td>
<td>40.1.1.24</td>
<td></td>
<td>200</td>
</tr>
<tr>
<td>Gi1/0/3</td>
<td>ip trk</td>
<td>active</td>
<td>40.1.1.20</td>
<td></td>
<td>200</td>
</tr>
<tr>
<td>Gi1/0/3</td>
<td>ip trk</td>
<td>active</td>
<td>40.1.1.21</td>
<td></td>
<td>200</td>
</tr>
<tr>
<td>Gi1/0/3</td>
<td>ip trk</td>
<td>active</td>
<td>40.1.1.22</td>
<td></td>
<td>200</td>
</tr>
<tr>
<td>Gi1/0/3</td>
<td>ip trk</td>
<td>active</td>
<td>40.1.1.23</td>
<td></td>
<td>201</td>
</tr>
<tr>
<td>Gi1/0/3</td>
<td>ip trk</td>
<td>active</td>
<td>40.1.1.24</td>
<td></td>
<td>201</td>
</tr>
<tr>
<td>Gi1/0/3</td>
<td>ip trk</td>
<td>active</td>
<td>40.1.1.20</td>
<td></td>
<td>201</td>
</tr>
<tr>
<td>Gi1/0/3</td>
<td>ip trk</td>
<td>active</td>
<td>40.1.1.21</td>
<td></td>
<td>201</td>
</tr>
<tr>
<td>Gi1/0/3</td>
<td>ip trk</td>
<td>active</td>
<td>40.1.1.22</td>
<td></td>
<td>201</td>
</tr>
</tbody>
</table>

The output shows that the five valid IP-MAC bindings are on both the primary and secondary VLAN.

Displaying IP Source Guard Information

To display the IP source guard information, use one or more of the privileged EXEC commands in Table 21-3:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip source binding</td>
<td>Display the IP source bindings on a switch.</td>
</tr>
<tr>
<td>show ip verify source</td>
<td>Display the IP source guard configuration on the switch.</td>
</tr>
</tbody>
</table>

Understanding DHCP Server Port-Based Address Allocation

DHCP server port-based address allocation is a feature that enables DHCP to maintain the same IP address on an Ethernet switch port regardless of the attached device client identifier or client hardware address.

When Ethernet switches are deployed in the network, they offer connectivity to the directly connected devices. In some environments, such as on a factory floor, if a device fails, the replacement device must be working immediately in the existing network. With the current DHCP implementation, there is no guarantee that DHCP would offer the same IP address to the replacement device. Control, monitoring, and other software expect a stable IP address associated with each device. If a device is replaced, the address assignment should remain stable even though the DHCP client has changed.

When configured, the DHCP server port-based address allocation feature ensures that the same IP address is always offered to the same connected port even as the client identifier or client hardware address changes in the DHCP messages received on that port. The DHCP protocol recognizes DHCP clients by the client identifier option in the DHCP packet. Clients that do not include the client identifier option are identified by the client hardware address. When you configure this feature, the port name of the interface overrides the client identifier or hardware address and the actual point of connection, the switch port, becomes the client identifier.

In all cases, by connecting the Ethernet cable to the same port, the same IP address is allocated through DHCP to the attached device.
The DHCP server port-based address allocation feature is only supported on a Cisco IOS DHCP server and not a third-party server.

## Configuring DHCP Server Port-Based Address Allocation

This section contains this configuration information:
- Default Port-Based Address Allocation Configuration, page 21-26
- Port-Based Address Allocation Configuration Guidelines, page 21-26
- Enabling DHCP Server Port-Based Address Allocation, page 21-26

### Default Port-Based Address Allocation Configuration

By default, DHCP server port-based address allocation is disabled.

### Port-Based Address Allocation Configuration Guidelines

These are the configuration guidelines for DHCP port-based address allocation:
- Only one IP address can be assigned per port.
- Reserved addresses (preassigned) cannot be cleared by using the `clear ip dhcp binding` global configuration command.
- Preassigned addresses are automatically excluded from normal dynamic IP address assignment. Preassigned addresses cannot be used in host pools, but there can be multiple preassigned addresses per DHCP address pool.
- To restrict assignments from the DHCP pool to preconfigured reservations (unreserved addresses are not offered to the client and other clients are not served by the pool), you can enter the `reserved-only` DHCP pool configuration command.

### Enabling DHCP Server Port-Based Address Allocation

Beginning in privileged EXEC mode, follow these steps to globally enable port-based address allocation and to automatically generate a subscriber identifier on an interface.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>ip dhcp use subscriber-id client-id</code></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>ip dhcp subscriber-id interface-name</code></td>
</tr>
</tbody>
</table>
Configuring DHCP Server Port-Based Address Allocation

After enabling DHCP port-based address allocation on the switch, use the `ip dhcp pool` global configuration command to preassign IP addresses and to associate them to clients. To restrict assignments from the DHCP pool to preconfigured reservations, you can enter the `reserved-only` DHCP pool configuration command. Unreserved addresses that are part of the network or on pool ranges are not offered to the client, and other clients are not served by the pool. By entering this command, users can configure a group of switches with DHCP pools that share a common IP subnet and that ignore requests from clients of other switches.

Beginning in privileged EXEC mode follow these steps to preassign an IP address and to associate it to a client identified by the interface name.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong></td>
<td><code>interface interface-id</code> Specify the interface to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>ip dhcp server use subscriber-id client-id</code> Configure the DHCP server to use the subscriber identifier as the client identifier on all incoming DHCP messages on the interface.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>end</code> Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><code>show running-config</code> Verify your entries.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><code>copy running-config startup-config</code> (Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable DHCP port-based address allocation, use the `no ip dhcp use subscriber-id client-id` global configuration command. To disable the automatic generation of a subscriber identifier, use the `no ip dhcp subscriber-id interface-name` global configuration command. To disable the subscriber identifier on an interface, use the `no ip dhcp server use subscriber-id client-id` interface configuration command.
To remove an IP address reservation from a DHCP pool, use the `no address ip-address client-id string` DHCP pool configuration command. To change the address pool to nonrestricted, enter the `no reserved-only` DHCP pool configuration command.

In this example, a subscriber identifier is automatically generated, and the DHCP server ignores any client identifier fields in the DHCP messages and uses the subscriber identifier instead. The subscriber identifier is based on the short name of the interface and the client preassigned IP address 10.1.1.7.

```
switch# show running config
Building configuration...
Current configuration : 4899 bytes
!
version 12.2
!
hostname switch
!
no aaa new-model
clock timezone EST 0
ip subnet-zero
ip dhcp relay information policy removal pad
no ip dhcp use vrf connected
ip dhcp use subscriber-id client-id
ip dhcp subscriber-id interface-name
ip dhcp excluded-address 10.1.1.1 10.1.1.3
!
ip dhcp pool dhcppool
    network 10.1.1.0 255.255.255.0
    address 10.1.1.7 client-id "Et1/0" ascii
<output truncated>
```

This example shows that the preassigned address was correctly reserved in the DHCP pool:

```
switch# show ip dhcp pool dhcppool
Pool dhcppool:
    Utilization mark (high/low) : 100 / 0
    Subnet size (first/next) : 0 / 0
    Total addresses : 254
    Leased addresses : 0
    Excluded addresses : 4
    Pending event : none
1 subnet is currently in the pool:
    Current index   IP address range         Leased/Excluded/Total
    10.1.1.1        10.1.1.1 - 10.1.1.254     0     / 4 / 254
1 reserved address is currently in the pool
    Address         Client
    10.1.1.7 Et1/0
```

For more information about configuring the DHCP server port-based address allocation feature, go to Cisco.com, and enter *Cisco IOS IP Addressing Services* in the Search field to access the Cisco IOS software documentation. You can also access the documentation here:

Displaying DHCP Server Port-Based Address Allocation

To display the DHCP server port-based address allocation information, use one or more of the privileged EXEC commands in Table 21-4:

**Table 21-4 Commands for Displaying DHCP Port-Based Address Allocation Information**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show interface interface id</code></td>
<td>Display the status and configuration of a specific interface.</td>
</tr>
<tr>
<td><code>show ip dhcp pool</code></td>
<td>Display the DHCP address pools.</td>
</tr>
<tr>
<td><code>show ip dhcp binding</code></td>
<td>Display address bindings on the Cisco IOS DHCP server.</td>
</tr>
</tbody>
</table>
Configuring Dynamic ARP Inspection

This chapter describes how to configure dynamic Address Resolution Protocol inspection (dynamic ARP inspection) on the Catalyst 3750 Metro switch. This feature helps prevent malicious attacks on the switch by not relaying invalid ARP requests and responses to other ports in the same VLAN.

Note

For complete syntax and usage information for the commands used in this chapter, see the command reference for this release.

This chapter consists of these sections:

- Understanding Dynamic ARP Inspection, page 22-1
- Configuring Dynamic ARP Inspection, page 22-5
- Displaying Dynamic ARP Inspection Information, page 22-14

Understanding Dynamic ARP Inspection

ARP provides IP communication within a Layer 2 broadcast domain by mapping an IP address to a MAC address. For example, Host B wants to send information to Host A but does not have the MAC address of Host A in its ARP cache. Host B generates a broadcast message for all hosts within the broadcast domain to obtain the MAC address associated with the IP address of Host A. All hosts within the broadcast domain receive the ARP request, and Host A responds with its MAC address. However, because ARP allows a gratuitous reply from a host even if an ARP request was not received, an ARP spoofing attack and the poisoning of ARP caches can occur. After the attack, all traffic from the device under attack flows through the attacker’s computer and then to the router, switch, or host.

A malicious user can attack hosts, switches, and routers connected to your Layer 2 network by poisoning the ARP caches of systems connected to the subnet and by intercepting traffic intended for other hosts on the subnet. Figure 22-1 shows an example of ARP cache poisoning.
Understanding Dynamic ARP Inspection

Figure 22-1  ARP Cache Poisoning

Host A  
(IA, MA)

A

Host C  
(man-in-the-middle)  
(IC, MC)

B

Host B  
(IB, MB)

Hosts A, B, and C are connected to the switch on interfaces A, B and C, all of which are on the same subnet. Their IP and MAC addresses are shown in parentheses; for example, Host A uses IP address IA and MAC address MA. When Host A needs to communicate to Host B at the IP layer, it broadcasts an ARP request for the MAC address associated with IP address IB. When the switch and Host B receive the ARP request, they populate their ARP caches with an ARP binding for a host with the IP address IA and a MAC address MA; for example, IP address IA is bound to MAC address MA. When Host B responds, the switch and Host A populate their ARP caches with a binding for a host with the IP address IB and the MAC address MB.

Host C can poison the ARP caches of the switch, Host A, and Host B by broadcasting forged ARP responses with bindings for a host with an IP address of IA (or IB) and a MAC address of MC. Hosts with poisoned ARP caches use the MAC address MC as the destination MAC address for traffic intended for IA or IB. This means that Host C intercepts that traffic. Because Host C knows the true MAC addresses associated with IA and IB, it can forward the intercepted traffic to those hosts by using the correct MAC address as the destination. Host C has inserted itself into the traffic stream from Host A to Host B, the classic man-in-the-middle attack.

Dynamic ARP inspection is a security feature that validates ARP packets in a network. It intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. This capability protects the network from certain man-in-the-middle attacks.

Dynamic ARP inspection ensures that only valid ARP requests and responses are relayed. The switch performs these activities:

- Intercepts all ARP requests and responses on untrusted ports
- Verifies that each of these intercepted packets has a valid IP-to-MAC address binding before updating the local ARP cache or before forwarding the packet to the appropriate destination
- Drops invalid ARP packets

Dynamic ARP inspection determines the validity of an ARP packet based on valid IP-to-MAC address bindings stored in a trusted database, the DHCP snooping binding database. This database is built by DHCP snooping if DHCP snooping is enabled on the VLANs and on the switch. If the ARP packet is received on a trusted interface, the switch forwards the packet without any checks. On untrusted interfaces, the switch forwards the packet only if it is valid.

You enable dynamic ARP inspection on a per-VLAN basis by using the \texttt{ip arp inspection vlan vlan-range} global configuration command. For configuration information, see the “Configuring Dynamic ARP Inspection in DHCP Environments” section on page 22-7.

In non-DHCP environments, dynamic ARP inspection can validate ARP packets against user-configured ARP access control lists (ACLs) for hosts with statically configured IP addresses. You define an ARP ACL by using the \texttt{arp access-list acl-name} global configuration command. For configuration information, see the “Configuring ARP ACLs for Non-DHCP Environments” section on page 22-8. The switch logs dropped packets. For more information about the log buffer, see the “Logging of Dropped Packets” section on page 22-4.
You can configure dynamic ARP inspection to drop ARP packets when the IP addresses in the packets are invalid or when the MAC addresses in the body of the ARP packets do not match the addresses specified in the Ethernet header. Use the `ip arp inspection validate {[src-mac] [dst-mac] [ip]}` global configuration command. For more information, see the “Performing Validation Checks” section on page 22-11.

**Interface Trust States and Network Security**

Dynamic ARP inspection associates a trust state with each interface on the switch. Packets arriving on trusted interfaces bypass all dynamic ARP inspection validation checks, and those arriving on untrusted interfaces undergo the dynamic ARP inspection validation process.

In a typical network configuration, you configure all switch ports connected to host ports as untrusted and configure all switch ports connected to switches as trusted. With this configuration, all ARP packets entering the network from a given switch bypass the security check. No other validation is needed at any other place in the VLAN or in the network. You configure the trust setting by using the `ip arp inspection trust` interface configuration command.

**Caution**

Use the trust state configuration carefully. Configuring interfaces as untrusted when they should be trusted can result in a loss of connectivity.

In Figure 22-2, assume that both Switch A and Switch B are running dynamic ARP inspection on the VLAN that includes Host 1 and Host 2. If Host 1 and Host 2 acquire their IP addresses from the DHCP server connected to Switch A, only Switch A binds the IP-to-MAC address of Host 1. Therefore, if the interface between Switch A and Switch B is untrusted, the ARP packets from Host 1 are dropped by Switch B. Connectivity between Host 1 and Host 2 is lost.

**Figure 22-2 ARP Packet Validation on a VLAN Enabled for Dynamic ARP Inspection**

Configuring interfaces to be trusted when they are actually untrusted leaves a security hole in the network. If Switch A is not running dynamic ARP inspection, Host 1 can easily poison the ARP cache of Switch B (and Host 2, if the link between the switches is configured as trusted). This condition can occur even though Switch B is running dynamic ARP inspection.
Understanding Dynamic ARP Inspection

Dynamic ARP inspection ensures that hosts (on untrusted interfaces) connected to a switch running dynamic ARP inspection do not poison the ARP caches of other hosts in the network. However, dynamic ARP inspection does not prevent hosts in other portions of the network from poisoning the caches of the hosts that are connected to a switch running dynamic ARP inspection.

In cases in which some switches in a VLAN run dynamic ARP inspection and other switches do not, configure the interfaces connecting such switches as untrusted. However, to validate the bindings of packets from nondynamic ARP inspection switches, configure the switch running dynamic ARP inspection with ARP ACLs. When you cannot determine such bindings, at Layer 3, isolate switches running dynamic ARP inspection from switches not running dynamic ARP inspection switches. For configuration information, see the “Configuring ARP ACLs for Non-DHCP Environments” section on page 22-8.

Note

Depending on the setup of the DHCP server and the network, it might not be possible to validate a given ARP packet on all switches in the VLAN.

Rate Limiting of ARP Packets

The switch CPU performs dynamic ARP inspection validation checks; therefore, the number of incoming ARP packets is rate-limited to prevent a denial-of-service attack. By default, the rate for untrusted interfaces is 15 packets per second (pps). Trusted interfaces are not rate-limited. You can change this setting by using the `ip arp inspection limit` interface configuration command.

When the rate of incoming ARP packets exceeds the configured limit, the switch places the port in the error-disabled state. The port remains in that state until you change it. You can use the `errdisable recovery` global configuration command to enable error disable recovery so that ports automatically emerge from this state after a specified timeout period.

For configuration information, see the “Limiting the Rate of Incoming ARP Packets” section on page 22-10.

Relative Priority of ARP ACLs and DHCP Snooping Entries

Dynamic ARP inspection uses the DHCP snooping binding database for the list of valid IP-to-MAC address bindings.

ARP ACLs take precedence over entries in the DHCP snooping binding database. The switch uses ACLs only if you configure them by using the `ip arp inspection filter vlan` global configuration command. The switch first compares ARP packets to user-configured ARP ACLs. If the ARP ACL denies the ARP packet, the switch also denies the packet even if a valid binding exists in the database populated by DHCP snooping.

Logging of Dropped Packets

When the switch drops a packet, it places an entry in the log buffer and then generates system messages on a rate-controlled basis. After the message is generated, the switch clears the entry from the log buffer. Each log entry contains flow information, such as the receiving VLAN, the port number, the source and destination IP addresses, and the source and destination MAC addresses.
You use the `ip arp inspection log-buffer` global configuration command to configure the number of entries in the buffer and the number of entries needed in the specified interval to generate system messages. You specify the type of packets that are logged by using the `ip arp inspection vlan logging` global configuration command. For configuration information, see the “Configuring the Log Buffer” section on page 22-12.

### Configuring Dynamic ARP Inspection

These sections describe how to configure dynamic ARP inspection on your switch:

- Default Dynamic ARP Inspection Configuration, page 22-5
- Dynamic ARP Inspection Configuration Guidelines, page 22-6
- Configuring Dynamic ARP Inspection in DHCP Environments, page 22-7 (required in DHCP environments)
- Configuring ARP ACLs for Non-DHCP Environments, page 22-8 (required in non-DHCP environments)
- Limiting the Rate of Incoming ARP Packets, page 22-10 (optional)
- Performing Validation Checks, page 22-11 (optional)
- Configuring the Log Buffer, page 22-12 (optional)

### Default Dynamic ARP Inspection Configuration

Table 22-1 shows the default dynamic ARP inspection configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic ARP inspection</td>
<td>Disabled on all VLANs.</td>
</tr>
<tr>
<td>Interface trust state</td>
<td>All interfaces are untrusted.</td>
</tr>
<tr>
<td>Rate limit of incoming ARP packets</td>
<td>The rate is 15 pps on untrusted interfaces, assuming that the network is a switched network with a host connecting to as many as 15 new hosts per second. The rate is unlimited on all trusted interfaces. The burst interval is 1 second.</td>
</tr>
<tr>
<td>ARP ACLs for non-DHCP environments</td>
<td>No ARP ACLs are defined.</td>
</tr>
<tr>
<td>Validation checks</td>
<td>No checks are performed.</td>
</tr>
<tr>
<td>Log buffer</td>
<td>When dynamic ARP inspection is enabled, all denied or dropped ARP packets are logged. The number of entries in the log is 32. The number of system messages is limited to 5 per second. The logging-rate interval is 1 second.</td>
</tr>
<tr>
<td>Per-VLAN logging</td>
<td>All denied or dropped ARP packets are logged.</td>
</tr>
</tbody>
</table>
Dynamic ARP Inspection Configuration Guidelines

These are the dynamic ARP inspection configuration guidelines:

- Dynamic ARP inspection is an ingress security feature; it does not perform any egress checking.
- Dynamic ARP inspection is not effective for hosts connected to switches that do not support dynamic ARP inspection or that do not have this feature enabled. Because man-in-the-middle attacks are limited to a single Layer 2 broadcast domain, separate the domain with dynamic ARP inspection checks from the one with no checking. This action secures the ARP caches of hosts in the domain enabled for dynamic ARP inspection.
- Dynamic ARP inspection depends on the entries in the DHCP snooping binding database to verify IP-to-MAC address bindings in incoming ARP requests and ARP responses. Make sure to enable DHCP snooping to permit ARP packets that have dynamically assigned IP addresses. For configuration information, see Chapter 21, “Configuring DHCP Features and IP Source Guard.” When DHCP snooping is disabled or in non-DHCP environments, use ARP ACLs to permit or to deny packets.
- Dynamic ARP inspection is supported on access ports, trunk ports, EtherChannel ports, and private VLAN ports.

**Note**

Do not enable Dynamic ARP inspection on RSPAN VLANs. If Dynamic ARP inspection is enabled on RSPAN VLANs, Dynamic ARP inspection packets might not reach the RSPAN destination port.

- A physical port can join an EtherChannel port channel only when the trust state of the physical port and the channel port match. Otherwise, the physical port remains suspended in the port channel. A port channel inherits its trust state from the first physical port that joins the channel. Consequently, the trust state of the first physical port need not match the trust state of the channel.

  Conversely, when you change the trust state on the port channel, the switch configures a new trust state on all the physical ports that comprise the channel.

- The rate limit is calculated separately on each switch in a switch stack. For a cross-stack EtherChannel, this means that the actual rate limit might be higher than the configured value. For example, if you set the rate limit to 30 pps on an EtherChannel that has one port on switch 1 and one port on switch 2, each port can receive packets at 29 pps without causing the EtherChannel to become error-disabled.

- The operating rate for the port channel is cumulative across all the physical ports within the channel. For example, if you configure the port channel with an ARP rate-limit of 400 pps, all the interfaces combined on the channel receive an aggregate 400 pps. The rate of incoming ARP packets on EtherChannel ports is equal to the sum of the incoming rate of packets from all the channel members. Configure the rate limit for EtherChannel ports only after examining the rate of incoming ARP packets on the channel-port members.

  The rate of incoming packets on a physical port is checked against the port-channel configuration rather than the physical-ports configuration. The rate-limit configuration on a port channel is independent of the configuration on its physical ports.

  If the EtherChannel receives more ARP packets than the configured rate, the channel (including all physical ports) is placed in the error-disabled state.
• Make sure to limit the rate of ARP packets on incoming trunk ports. Configure trunk ports with higher rates to reflect their aggregation and to handle packets across multiple dynamic ARP inspection-enabled VLANs. You also can use the `ip arp inspection limit none` interface configuration command to make the rate unlimited. A high rate-limit on one VLAN can cause a denial-of-service attack to other VLANs when the software places the port in the error-disabled state.

• When you enable dynamic ARP inspection on the switch, policers that were configured to police ARP traffic are no longer effective. The result is that all ARP traffic is sent to the CPU.

## Configuring Dynamic ARP Inspection in DHCP Environments

This procedure shows how to configure dynamic ARP inspection when two switches support this feature. Host 1 is connected to Switch A, and Host 2 is connected to Switch B as shown in Figure 22-2 on page 22-3. Both switches are running dynamic ARP inspection on VLAN 1 where the hosts are located. A DHCP server is connected to Switch A. Both hosts acquire their IP addresses from the same DHCP server. Therefore, Switch A has the bindings for Host 1 and Host 2, and Switch B has the binding for Host 2.

**Note**
Dynamic ARP inspection depends on the entries in the DHCP snooping binding database to verify IP-to-MAC address bindings in incoming ARP requests and ARP responses. Make sure to enable DHCP snooping to permit ARP packets that have dynamically assigned IP addresses. For configuration information, see Chapter 21, “Configuring DHCP Features and IP Source Guard.”

For information on how to configure dynamic ARP inspection when only one switch supports the feature, see the “Configuring ARP ACLs for Non-DHCP Environments” section on page 22-8.

Beginning in privileged EXEC mode, follow these steps to configure dynamic ARP inspection. You must perform this procedure on both switches. This procedure is required.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>show cdp neighbors</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>ip arp inspection vlan vlan-range</code></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>interface interface-id</code></td>
</tr>
</tbody>
</table>
Chapter 22 Configuring Dynamic ARP Inspection

Configuring Dynamic ARP Inspection

To disable dynamic ARP inspection, use the `no ip arp inspection vlan VLAN-Range` global configuration command. To return the interfaces to an untrusted state, use the `no ip arp inspection trust INTERFACE` command.

This example shows how to configure dynamic ARP inspection on Switch A in VLAN 1. You would perform a similar procedure on Switch B:

```
Switch(config)# ip arp inspection vlan 1
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip arp inspection trust
```

### Configuring ARP ACLs for Non-DHCP Environments

This procedure shows how to configure dynamic ARP inspection when Switch B shown in Figure 22-2 on page 22-3 does not support dynamic ARP inspection or DHCP snooping.

If you configure port 1 on Switch A as trusted, a security hole is created because both Switch A and Host 1 could be attacked by either Switch B or Host 2. To prevent this possibility, you must configure port 1 on Switch A as untrusted. To permit ARP packets from Host 2, you must set up an ARP ACL and apply it to VLAN 1. If the IP address of Host 2 is not static (it is impossible to apply the ACL configuration on Switch A) you must separate Switch A from Switch B at Layer 3 and use a router to route packets between them.
Beginning in privileged EXEC mode, follow these steps to configure an ARP ACL on Switch A. This procedure is required in non-DHCP environments.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 arp access-list acl-name</td>
<td>Define an ARP ACL, and enter ARP access-list configuration mode. By default, no ARP access lists are defined.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>At the end of the ARP access list, there is an implicit <strong>deny ip any mac any</strong> command.</td>
</tr>
<tr>
<td>Step 3 permit ip host sender-ip mac host sender-mac [log]</td>
<td>Permit ARP packets from the specified host (Host 2).</td>
</tr>
<tr>
<td></td>
<td>• For <em>sender-ip</em>, enter the IP address of Host 2.</td>
</tr>
<tr>
<td></td>
<td>• For <em>sender-mac</em>, enter the MAC address of Host 2.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) Specify <em>log</em> to log a packet in the log buffer when it matches the access control entry (ACE). Matches are logged if you also configure the <em>matchlog</em> keyword in the <strong>ip arp inspection vlan logging</strong> global configuration command. For more information, see the “Configuring the Log Buffer” section on page 22-12.</td>
</tr>
<tr>
<td>Step 4 exit</td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td>Step 5 ip arp inspection filter arp-acl-name vlan vlan-range [static]</td>
<td>Apply the ARP ACL to the VLAN. By default, no defined ARP ACLs are applied to any VLAN.</td>
</tr>
<tr>
<td></td>
<td>• For <em>arp-acl-name</em>, specify the name of the ACL created in Step 2.</td>
</tr>
<tr>
<td></td>
<td>• For <em>vlan-range</em>, specify the VLAN that the switches and hosts are in. You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) Specify <em>static</em> to treat implicit denies in the ARP ACL as explicit denies and to drop packets that do not match any previous clauses in the ACL. DHCP bindings are not used. If you do not specify this keyword, it means that there is no explicit deny in the ACL that denies the packet, and DHCP bindings determine whether a packet is permitted or denied if the packet does not match any clauses in the ACL. ARP packets containing only IP-to-MAC address bindings are compared against the ACL. Packets are permitted only if the access list permits them.</td>
</tr>
<tr>
<td>Step 6 interface interface-id</td>
<td>Specify the Switch A interface that is connected to Switch B, and enter interface configuration mode.</td>
</tr>
</tbody>
</table>
### Configuring Dynamic ARP Inspection

#### Command

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td><code>no ip arp inspection trust</code></td>
<td>Configure the Switch A interface that is connected to Switch B as untrusted. By default, all interfaces are untrusted. For untrusted interfaces, the switch intercepts all ARP requests and responses. It verifies that the intercepted packets have valid IP-to-MAC address bindings before updating the local cache and before forwarding the packet to the appropriate destination. The switch drops invalid packets and logs them in the log buffer according to the logging configuration specified with the <code>ip arp inspection vlan logging</code> global configuration command. For more information, see the “Configuring the Log Buffer” section on page 22-12.</td>
</tr>
<tr>
<td>8</td>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
| 9    | `show arp access-list [acl-name]`  
`show ip arp inspection vlan [vlan-range]`  
`show ip arp inspection interfaces` | Verify your entries. |
| 10   | `copy running-config startup-config` | (Optional) Save your entries in the configuration file. |

To remove the ARP ACL, use the `no arp access-list` global configuration command. To remove the ARP ACL attached to a VLAN, use the `no ip arp inspection filter [arp-acl-name] [vlan] [vlan-range]` global configuration command.

This example shows how to configure an ARP ACL called `host2` on Switch A, to permit ARP packets from Host 2 (IP address 1.1.1.1 and MAC address 0001.0001.0001), to apply the ACL to VLAN 1, and to configure port 1 on Switch A as untrusted:

```plaintext
Switch(config)# arp access-list host2
Switch(config-arp-acl)# permit ip host 1.1.1.1 mac host 1.1.1
Switch(config-arp-acl)# exit
Switch(config)# ip arp inspection filter host2 [vlan] 1
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# no ip arp inspection trust
```

### Limiting the Rate of Incoming ARP Packets

The switch CPU performs dynamic ARP inspection validation checks; therefore, the number of incoming ARP packets is rate-limited to prevent a denial-of-service attack.

When the rate of incoming ARP packets exceeds the configured limit, the switch places the port in the error-disabled state. The port remains in that state until you enable error-disable recovery so that ports automatically emerge from this state after a specified timeout period.

**Note**

Unless you configure a rate limit on an interface, changing the trust state of the interface also changes its rate limit to the default value for that trust state. After you configure the rate limit, the interface retains the rate limit even when its trust state is changed. If you enter the `no ip arp inspection limit` interface configuration command, the interface reverts to its default rate limit.
Configuring Dynamic ARP Inspection

For configuration guidelines for rate limiting trunk ports and EtherChannel ports, see the “Dynamic ARP Inspection Configuration Guidelines” section on page 22-6.

Beginning in privileged EXEC mode, follow these steps to limit the rate of incoming ARP packets. This procedure is optional.

### Command Purpose

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>interface interface-id</td>
<td>Specify the interface to be rate-limited, and enter interface configuration mode.</td>
</tr>
<tr>
<td>3</td>
<td>ip arp inspection limit { rate pps [burst interval seconds]</td>
<td>Limit the rate of incoming ARP requests and responses on the interface. The default rate is 15 pps on untrusted interfaces and unlimited on trusted interfaces. The burst interval is 1 second. The keywords have these meanings:</td>
</tr>
<tr>
<td></td>
<td>none }</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- For rate pps, specify an upper limit for the number of incoming packets processed per second. The range is 0 to 2048 pps.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- (Optional) For burst interval seconds, specify the consecutive interval in seconds, over which the interface is monitored for a high rate of ARP packets. The range is 1 to 15.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- For rate none, specify no upper limit for the rate of incoming ARP packets that can be processed.</td>
</tr>
<tr>
<td>4</td>
<td>exit</td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td>5</td>
<td>errdisable recovery cause arp-inspection interval interval</td>
<td>(Optional) Enable error recovery from the dynamic ARP inspection error-disable state. By default, recovery is disabled, and the recovery interval is 300 seconds. For interval interval, specify the time in seconds to recover from the error-disable state. The range is 30 to 86400.</td>
</tr>
<tr>
<td>6</td>
<td>exit</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>7</td>
<td>show ip arp inspection interfaces</td>
<td>Verify your settings.</td>
</tr>
<tr>
<td>8</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default rate-limit configuration, use the no ip arp inspection limit interface configuration command. To disable error recovery for dynamic ARP inspection, use the no errdisable recovery cause arp-inspection global configuration command.

### Performing Validation Checks

Dynamic ARP inspection intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. You can configure the switch to perform additional checks on the destination MAC address, the sender and target IP addresses, and the source MAC address.
Beginning in privileged EXEC mode, follow these steps to perform specific checks on incoming ARP packets. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip arp inspection validate [[src-mac] [dst-mac] [ip]]</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>exit</td>
</tr>
<tr>
<td>Step 4</td>
<td>show ip arp inspection vlan vlan-range</td>
</tr>
<tr>
<td>Step 5</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To disable checking, use the `no ip arp inspection validate [src-mac] [dst-mac] [ip]` global configuration command. To display statistics for forwarded, dropped, and MAC and IP validation failure packets, use the `show ip arp inspection statistics` privileged EXEC command.

### Configuring the Log Buffer

When the switch drops a packet, it places an entry in the log buffer and then generates system messages on a rate-controlled basis. After the message is generated, the switch clears the entry from the log buffer. Each log entry contains flow information, such as the receiving VLAN, the port number, the source and destination IP addresses, and the source and destination MAC addresses.

A log-buffer entry can represent more than one packet. For example, if an interface receives many packets on the same VLAN with the same ARP parameters, the switch combines the packets as one entry in the log buffer and generates a single system message for the entry.
If the log buffer overflows, it means that a log event does not fit into the log buffer, and the display for the `show ip arp inspection log` privileged EXEC command is affected. A -- in the display appears in place of all data except the packet count and the time. No other statistics are provided for the entry. If you see this entry in the display, increase the number of entries in the log buffer or increase the logging rate.

Beginning in privileged EXEC mode, follow these steps to configure the log buffer. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>configure terminal</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Configure the dynamic ARP inspection logging buffer.</td>
</tr>
<tr>
<td>`ip arp inspection log-buffer {entries number</td>
<td>By default, when dynamic ARP inspection is enabled, denied or dropped</td>
</tr>
<tr>
<td>logs number interval seconds}</td>
<td>ARP packets are logged. The number of log entries is 32. The number</td>
</tr>
<tr>
<td></td>
<td>of system messages is limited to 5 per second. The logging-rate interval</td>
</tr>
<tr>
<td></td>
<td>is 1 second.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The keywords have these meanings:</td>
</tr>
<tr>
<td></td>
<td>• For <code>entries number</code>, specify the number of entries to be logged in</td>
</tr>
<tr>
<td></td>
<td>the buffer. The range is 0 to 1024.</td>
</tr>
<tr>
<td></td>
<td>• For <code>logs number interval seconds</code>, specify the number of entries to</td>
</tr>
<tr>
<td></td>
<td>generate system messages in the specified interval.</td>
</tr>
<tr>
<td></td>
<td>For <code>logs number</code>, the range is 0 to 1024. A 0 value means that the</td>
</tr>
<tr>
<td></td>
<td>entry is placed in the log buffer, but a system message is not</td>
</tr>
<tr>
<td></td>
<td>generated.</td>
</tr>
<tr>
<td></td>
<td>For <code>interval seconds</code>, the range is 0 to 86400 seconds (1 day). A 0</td>
</tr>
<tr>
<td></td>
<td>value means that a system message is immediately generated (and the</td>
</tr>
<tr>
<td></td>
<td>log buffer is always empty).</td>
</tr>
<tr>
<td></td>
<td>An interval setting of 0 overrides a log setting of 0.</td>
</tr>
<tr>
<td></td>
<td>The <code>logs</code> and <code>interval</code> settings interact. If the <code>logs number X</code> is</td>
</tr>
<tr>
<td></td>
<td>greater than <code>interval seconds Y</code>, <code>X</code> divided by <code>Y (X/Y)</code> system</td>
</tr>
<tr>
<td></td>
<td>messages are sent every second. Otherwise, one system message is</td>
</tr>
<tr>
<td></td>
<td>sent every <code>Y</code> divided by <code>X (Y/X)</code> seconds.</td>
</tr>
</tbody>
</table>
Displaying Dynamic ARP Inspection Information

To display dynamic ARP inspection information, use the privileged EXEC commands described in Table 22-2:

**Table 22-2 Commands for Displaying Dynamic ARP Inspection Information**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show arp access-list [acl-name]</td>
<td>Displays detailed information about ARP ACLs.</td>
</tr>
<tr>
<td>show ip arp inspection interfaces [interface-id]</td>
<td>Displays the trust state and the rate limit of ARP packets for the specified interface or all interfaces.</td>
</tr>
<tr>
<td>show ip arp inspection vlan vlan-range</td>
<td>Displays the configuration and the operating state of dynamic ARP inspection for the specified VLAN. If no VLANs are specified or if a range is specified, displays information only for VLANs with dynamic ARP inspection enabled (active).</td>
</tr>
</tbody>
</table>
To clear or display dynamic ARP inspection statistics, use the privileged EXEC commands in Table 22-3:

Table 22-3 Commands for Clearing or Displaying Dynamic ARP Inspection Statistics

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip arp inspection statistics</td>
<td>Clears dynamic ARP inspection statistics.</td>
</tr>
<tr>
<td>show ip arp inspection statistics [vlan vlan-range]</td>
<td>Displays statistics for forwarded, dropped, MAC validation failure, IP validation failure, ACL permitted and denied, and DHCP permitted and denied packets for the specified VLAN. If no VLANs are specified or if a range is specified, displays information only for VLANs with dynamic ARP inspection enabled (active).</td>
</tr>
</tbody>
</table>

For the show ip arp inspection statistics command, the switch increments the number of forwarded packets for each ARP request and response packet on a trusted dynamic ARP inspection port. The switch increments the number of ACL or DHCP permitted packets for each packet that is denied by source MAC, destination MAC, or IP validation checks, and the switch increments the appropriate failure count.

To clear or display dynamic ARP inspection logging information, use the privileged EXEC commands in Table 22-4:

Table 22-4 Commands for Clearing or Displaying Dynamic ARP Inspection Logging Information

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip arp inspection log</td>
<td>Clears the dynamic ARP inspection log buffer.</td>
</tr>
<tr>
<td>show ip arp inspection log</td>
<td>Displays the configuration and contents of the dynamic ARP inspection log buffer.</td>
</tr>
</tbody>
</table>

For more information about these commands, see the command reference for this release.
Configuring IGMP Snooping and MVR

This chapter describes how to configure Internet Group Management Protocol (IGMP) snooping on the Catalyst 3750 Metro switch, including an application of local IGMP snooping, Multicast VLAN Registration (MVR). It also includes procedures for controlling multicast group membership by using IGMP filtering.

Note
For complete syntax and usage information for the commands used in this chapter, see the switch command reference for this release and the “IP Multicast Routing Commands” section in the Cisco IOS IP Command Reference, Volume 3 of 3: Multicast, Release 12.2.

This chapter consists of these sections:
- Understanding IGMP Snooping, page 23-1
- Configuring IGMP Snooping, page 23-5
- Displaying IGMP Snooping Information, page 23-12
- Understanding Multicast VLAN Registration, page 23-13
- Configuring MVR, page 23-16
- Displaying MVR Information, page 23-21
- Configuring IGMP Filtering and Throttling, page 23-21
- Displaying IGMP Filtering and Throttling Configuration, page 23-26

Note
You can either manage IP multicast group addresses through features such as IGMP snooping and MVR, or you can use static IP addresses.

Understanding IGMP Snooping

Layer 2 switches can use IGMP snooping to constrain the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded to only those interfaces associated with IP multicast devices. As the name implies, IGMP snooping requires the LAN switch to snoop on the IGMP transmissions between the host and the router and to keep track of multicast groups and member ports. When the switch receives an IGMP report from a host for a particular multicast group, the switch adds the host port number to the forwarding table entry; when it receives an IGMP Leave Group message from a host, it removes the host port from the table entry. It also periodically deletes entries if it does not receive IGMP membership reports from the multicast clients.
Understanding IGMP Snooping

Note

For more information on IP multicast and IGMP, see RFC 1112 and RFC 2236.

The multicast router (which could be a Catalyst 3750 Metro switch) sends out periodic general queries to all VLANs. All hosts interested in this multicast traffic send join requests and are added to the forwarding table entry. The switch creates one entry per VLAN in the IGMP snooping IP multicast forwarding table for each group from which it receives an IGMP join request.

The switch supports IP multicast group-based bridging, rather than MAC-addressed based groups. With multicast MAC address-based groups, if an IP address being configured translates (aliases) to a previously configured MAC address or to any reserved multicast MAC addresses (in the range 224.0.0.xxx), the command fails. Because the switch uses IP multicast groups, there are no address aliasing issues.

The IP multicast groups learned through IGMP snooping are dynamic. However, you can statically configure multicast groups by using the `ip igmp snooping vlan vlan-id static ip_address interface interface-id` global configuration 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.

You can configure an IGMP snooping querier to support IGMP snooping in subnets without multicast interfaces because the multicast traffic does not need to be routed. For more information about the IGMP snooping querier, see the “Configuring the IGMP Snooping Querier” section on page 23-10.

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 deleted.

These sections describe characteristics of IGMP snooping on the switch:

- IGMP Versions, page 23-2
- Joining a Multicast Group, page 23-3
- Leaving a Multicast Group, page 23-4
- Immediate Leave, page 23-5

IGMP Versions

The switch supports IGMP Version 1, IGMP Version 2, and IGMP Version 3. These versions are interoperable on the switch. For example, if IGMP snooping is enabled on an IGMPv2 switch and the switch receives an IGMPv3 report from a host, the switch can forward the IGMPv3 report to the multicast router.

Note

The switch supports IGMPv3 snooping based only on the destination multicast MAC address. It does not support snooping based on the source MAC address or on proxy reports.

An IGMPv3 switch supports Basic IGMPv3 Snooping Support (BISS), which includes support for the snooping features on IGMPv1 and IGMPv2 switches and for IGMPv3 membership report messages. BISS constrains the flooding of multicast traffic when your network includes IGMPv3 hosts. It constrains traffic to approximately the same set of ports as the IGMP snooping feature on IGMPv2 or IGMPv1 hosts.

Note

IGMPv3 join and leave messages are not supported on switches running IGMP filtering or MVR.
An IGMPv3 switch can receive messages from and forward messages to a device running the Source Specific Multicast (SSM) feature. For more information about source-specific multicast with IGMPv3 and IGMP, see this URL:


### Joining a Multicast Group

When a host connected to the switch wants to join an IP multicast group, if it is an IGMP Version 2 client, it sends an unsolicited IGMP join message, specifying the IP multicast group to join. Alternatively, when the switch receives a general query from the router, it forwards the query to all ports in the VLAN. IGMP Version 1 or Version 2 hosts wanting to join the multicast group respond by sending a join message to the switch. The switch CPU creates a multicast forwarding-table entry for the group if it is not already present. The CPU also adds the interface where the join message was received to the forwarding-table entry. The host associated with that interface receives multicast traffic for that multicast group. See Figure 23-1.

**Figure 23-1 Initial IGMP Join Message**

Router A sends a general query to the switch, which forwards the query to ports 2 through 5, all members of the same VLAN. Host 1 wants to join multicast group 224.1.2.3 and multicasts an IGMP membership report (IGMP join message) to the group. When the CPU receives the IGMP report multicast by Host 1, the CPU uses the information in the IGMP report to set up a forwarding-table entry, as shown in Table 23-1, that includes the port numbers connected to Host 1 and the router.

**Table 23-1 IGMP Snooping Forwarding Table**

<table>
<thead>
<tr>
<th>Destination Address</th>
<th>Type of Packet</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>224.1.2.3</td>
<td>IGMP</td>
<td>1, 2</td>
</tr>
</tbody>
</table>

The switch hardware can distinguish IGMP information packets from other packets for the multicast group. The information in the table tells the switching engine to send frames addressed to the 224.1.2.3 multicast IP address that are not IGMP packets to the router and to the host that has joined the group.
If another host (for example, Host 4) sends an unsolicited IGMP join message for the same group (Figure 23-2), the CPU receives that message and adds the port number of Host 4 to the forwarding table as shown in Table 23-2. Note that because the forwarding table directs IGMP messages only to the CPU, the message is not flooded to other ports on the switch. Any known multicast traffic is forwarded to the group and not to the CPU.

**Figure 23-2 Second Host Joining a Multicast Group**

![Image](image.png)

**Table 23-2 Updated IGMP Snooping Forwarding Table**

<table>
<thead>
<tr>
<th>Destination Address</th>
<th>Type of Packet</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>224.1.2.3</td>
<td>IGMP</td>
<td>1, 2, 5</td>
</tr>
</tbody>
</table>

**Leaving a Multicast Group**

The router sends periodic multicast general queries, and the switch forwards these queries through all ports in the VLAN. Interested hosts respond to the queries. If at least one host in the VLAN wishes to receive multicast traffic, the router continues forwarding the multicast traffic to the VLAN. The switch forwards multicast group traffic only to those hosts listed in the forwarding table for that IP multicast group maintained by IGMP snooping.

When hosts want to leave a multicast group, they can silently leave 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 learn if any other devices connected to that interface are interested in traffic for the specific multicast group. The switch then updates the forwarding table for that MAC group so that only those hosts interested in receiving multicast traffic for the group are listed in the forwarding table. If the router receives no reports from a VLAN, it removes the group for the VLAN from its IGMP cache.
Immediate Leave

Immediate Leave is only supported with IGMP Version 2 hosts.

The switch uses IGMP snooping Immediate-Leave processing to remove from the forwarding table an interface that sends a leave message without the switch sending group-specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Immediate-Leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are simultaneously in use.

---

**Note**

You should only use the Immediate-Leave processing feature on VLANs where a single host is connected to each port. If Immediate Leave is enabled in VLANs where more than one host is connected to a port, some hosts might be inadvertently dropped.

For configuration steps, see the “Enabling IGMP Immediate Leave” section on page 23-10.

IGMP Report Suppression

---

**Note**

IGMP report suppression is supported only when the multicast query has IGMPv1 and IGMPv2 reports. This feature is not supported when the query includes IGMPv3 reports.

The switch uses IGMP report suppression to forward only one IGMP report per multicast router query to multicast devices. When IGMP router suppression is enabled (the default), the switch sends the first IGMP report from all hosts blade servers for a group to all the multicast routers. The switch does not send the remaining IGMP reports for the group to the multicast routers. This feature prevents duplicate reports from being sent to the multicast devices.

If the multicast router query includes requests only for IGMPv1 and IGMPv2 reports, the switch forwards only the first IGMPv1 or IGMPv2 report from all hosts blade servers for a group to all the multicast routers.

If the multicast router query also includes requests for IGMPv3 reports, the switch forwards all IGMPv1, IGMPv2, and IGMPv3 reports for a group to the multicast devices.

If you disable IGMP report suppression, all IGMP reports are forwarded to the multicast routers. For configuration steps, see the “Disabling IGMP Report Suppression” section on page 23-12.

Configuring IGMP Snooping

IGMP snooping allows switches to examine IGMP packets and make forwarding decisions based on their content.

These sections describe how to configure IGMP snooping:

- Default IGMP Snooping Configuration, page 23-6
- Enabling or Disabling IGMP Snooping, page 23-6
- Setting the Snooping Method, page 23-7
- Configuring a Multicast Router Port, page 23-8
- Configuring a Host Statically to Join a Group, page 23-9
Default IGMP Snooping Configuration

Table 23-3 shows the default IGMP snooping configuration.

Table 23-3  Default IGMP Snooping Configuration

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP snooping</td>
<td>Enabled globally and per VLAN</td>
</tr>
<tr>
<td>Multicast routers</td>
<td>None configured</td>
</tr>
<tr>
<td>Multicast router learning (snooping) method</td>
<td>PIM-DVMRP</td>
</tr>
<tr>
<td>IGMP snooping Immediate Leave</td>
<td>Disabled</td>
</tr>
<tr>
<td>Static groups</td>
<td>None configured</td>
</tr>
<tr>
<td>IGMP snooping querier</td>
<td>Disabled</td>
</tr>
<tr>
<td>IGMP report suppression</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

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. IGMP snooping is by default enabled on all VLANs, but can be enabled and disabled on a per-VLAN basis.

Global IGMP snooping overrides the VLAN IGMP snooping. If global snooping is disabled, you cannot enable VLAN snooping. If global snooping is enabled, you can enable or disable VLAN snooping.

Beginning in privileged EXEC mode, follow these steps to globally enable IGMP snooping on the switch:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>ip igmp snooping</td>
<td>Globally enable IGMP snooping in all existing VLAN interfaces.</td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To globally disable IGMP snooping on all VLAN interfaces, use the `no ip igmp snooping` global configuration command.
Configuring IGMP Snooping and MVR

### Chapter 23

**Configuring IGMP Snooping**

Beginning in privileged EXEC mode, follow these steps to enable IGMP snooping on a VLAN interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>ip igmp snooping vlan <em>vlan-id</em></td>
<td>Enable IGMP snooping on the VLAN interface. The VLAN ID range is 1 to 1001 and 1006 to 4094. Note IGMP snooping must be globally enabled before you can enable VLAN snooping.</td>
</tr>
<tr>
<td>3</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>4</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable IGMP snooping on a VLAN interface, use the `no ip igmp snooping vlan *vlan-id*` global configuration command for the specified VLAN number.

### Setting the Snooping Method

Multicast-capable router ports are added to the forwarding table for every Layer 2 multicast entry. The switch learns of such ports through one of these methods:

- Snooping on IGMP queries, Protocol Independent Multicast (PIM) packets, and Distance Vector Multicast Routing Protocol (DVMRP) packets
- Listening to Cisco Group Management Protocol (CGMP) packets from other routers
- Statically connecting to a multicast router port with the `ip igmp snooping mrouter` global configuration command

You can configure the switch either to snoop on IGMP queries and PIM/DVMRP packets or to listen to CGMP self-join or proxy-join packets. By default, the switch snoops on PIM/DVMRP packets on all VLANs. To learn of multicast router ports through only CGMP packets, use the `ip igmp snooping vlan *vlan-id* mrouter learn cgmp` global configuration command. When this command is entered, the router listens to only CGMP self-join and CGMP proxy-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` global configuration command.

**Note**

If you want to use CGMP as the learning method and no multicast routers in the VLAN are CGMP proxy-enabled, you must enter the `ip cgmp router-only` command to dynamically access the router. For more information, see Chapter 45, “Configuring IP Multicast Routing.”
Beginning in privileged EXEC mode, follow these steps to alter the method in which a VLAN interface dynamically accesses a multicast router:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 ip igmp snooping vlan vlan-id mrouter learn {cgmp</td>
<td>pim-dvmrp}</td>
</tr>
<tr>
<td></td>
<td>• cgmp—Listen for CGMP packets. This method is useful for reducing control traffic.</td>
</tr>
<tr>
<td></td>
<td>• pim-dvmrp—Snoop on IGMP queries and PIM-DVMRP packets. This is the default.</td>
</tr>
<tr>
<td>Step 3 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4 show ip igmp snooping</td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td>Step 5 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default learning method, use the no ip igmp snooping vlan vlan-id mrouter learn cgmp global configuration command.

This example shows how to configure IGMP snooping to use CGMP packets as the learning method:

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 1 mrouter learn cgmp
Switch(config)# end
```

### Configuring a Multicast Router Port

To add a multicast router port (add a static connection to a multicast router), use the ip igmp snooping vlan mrouting global configuration command on the switch.

**Note** Static connections to multicast routers are supported only on switch ports.

Beginning in privileged EXEC mode, follow these steps to enable a static connection to a multicast router:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 ip igmp snooping vlan vlan-id mrouter interface interface-id</td>
<td>Specify the multicast router VLAN ID and specify the interface to the multicast router.</td>
</tr>
<tr>
<td></td>
<td>• The VLAN ID range is 1 to 1001 and 1006 to 4094.</td>
</tr>
<tr>
<td></td>
<td>• The interface can be a physical interface or a port channel. The port channel range is 1 to 12.</td>
</tr>
<tr>
<td>Step 3 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
Chapter 23 Configuring IGMP Snooping and MVR

Configuring IGMP Snooping

To remove a multicast router port from the VLAN, use the `no ip igmp snooping vlan vlan-id mrouter interface interface-id` global configuration command.

This example shows how to enable a static connection to a multicast router:

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 200 mrouter interface gigabitethernet1/0/2
Switch(config)# end
```

Configuring a Host Statically to Join a Group

Hosts or Layer 2 ports normally join multicast groups dynamically, but you can also statically configure a host on an interface.

Beginning in privileged EXEC mode, follow these steps to add a Layer 2 port as a member of a multicast group:

```
Step 1 configure terminal

Step 2 ip igmp snooping vlan vlan-id static ip_address interface interface-id

Step 3 end

Step 4 show ip igmp snooping groups

Step 5 copy running-config startup-config
```

To remove the Layer 2 port from the multicast group, use the `no ip igmp snooping vlan vlan-id static mac-address interface interface-id` global configuration command.

This example shows how to statically configure a host on an interface:

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 105 static 224.2.4.12 interface gigabitethernet1/0/1
Switch(config)# end
```
Enabling IGMP Immediate Leave

When you enable IGMP Immediate Leave, the switch immediately removes a port when it detects an IGMP Version 2 leave message on that port. You should use the Immediate-Leave feature only when there is a single receiver present on every port in the VLAN.

**Note**

Immediate Leave is supported with only IGMP Version 2 hosts.

Beginning in privileged EXEC mode, follow these steps to enable IGMP Immediate Leave:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode</td>
</tr>
<tr>
<td>Step 2 ip igmp snooping vlan vlan-id</td>
<td>Enable IGMP Immediate Leave on the VLAN interface.</td>
</tr>
<tr>
<td>immediate-leave</td>
<td></td>
</tr>
<tr>
<td>Step 3 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4 show ip igmp snooping vlan vlan-id</td>
<td>Verify that Immediate Leave is enabled on the VLAN.</td>
</tr>
<tr>
<td>Step 5 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable IGMP Immediate Leave on a VLAN, use the no ip igmp snooping vlan vlan-id immediate-leave global configuration command.

This example shows how to enable IGMP Immediate Leave on VLAN 130:

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 130 immediate-leave
Switch(config)# end
```

Configuring the IGMP Snooping Querier

Follow these guidelines when configuring the IGMP snooping querier:

- Configure the VLAN in global configuration mode.
- Configure an IP address on the VLAN interface. When enabled, the IGMP snooping querier uses the IP address as the query source address.
- If there is no IP address configured on the VLAN interface, the IGMP snooping querier tries to use the configured global IP address for the IGMP querier. If there is no global IP address specified, the IGMP querier tries to use the VLAN switch virtual interface (SVI) IP address (if one exists). If there is no SVI IP address, the switch uses the first available IP address configured on the switch. The first IP address available appears in the output of the show ip interface privileged EXEC command. The IGMP snooping querier does not generate an IGMP general query if it cannot find an available IP address on the switch.
- The IGMP snooping querier supports IGMP Versions 1 and 2.
- When administratively enabled, the IGMP snooping querier moves to the nonquerier state if it detects the presence of a multicast router in the network.
When it is administratively enabled, the IGMP snooping querier moves to the operationally disabled state under these conditions:

- IGMP snooping is disabled in the VLAN.
- PIM is enabled on the SVI of the corresponding VLAN.

Beginning in privileged EXEC mode, follow these steps to enable the IGMP snooping querier feature in a VLAN:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip igmp snooping querier</td>
</tr>
<tr>
<td>Step 3</td>
<td>ip igmp snooping querier address ip_address</td>
</tr>
<tr>
<td>Step 4</td>
<td>ip igmp snooping querier query-interval interval-count</td>
</tr>
<tr>
<td>Step 5</td>
<td>ip igmp snooping querier tcn query [count</td>
</tr>
<tr>
<td>Step 6</td>
<td>ip igmp snooping querier timer expiry timeout</td>
</tr>
<tr>
<td>Step 7</td>
<td>ip igmp snooping querier version version</td>
</tr>
<tr>
<td>Step 8</td>
<td>end</td>
</tr>
<tr>
<td>Step 9</td>
<td>show ip igmp snooping vlan vlan-id</td>
</tr>
<tr>
<td>Step 10</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

This example shows how to set the IGMP snooping querier source address to 10.0.0.64:
```
Switch# configure terminal
Switch(config)# ip igmp snooping querier 10.0.0.64
Switch(config)# end
```

This example shows how to set the IGMP snooping querier maximum response time to 25 seconds:
```
Switch# configure terminal
Switch(config)# ip igmp snooping querier query-interval 25
Switch(config)# end
```

This example shows how to set the IGMP snooping querier timeout to 60 seconds:
```
Switch# configure terminal
Switch(config)# ip igmp snooping querier timeout expiry 60
Switch(config)# end
```

This example shows how to set the IGMP snooping querier feature to version 2:
```
Switch# configure terminal
Switch(config)# no ip igmp snooping querier version 2
Switch(config)# end
```
Disabling IGMP Report Suppression

**Note**
IGMP report suppression is supported only when the multicast query has IGMPv1 and IGMPv2 reports. This feature is not supported when the query includes IGMPv3 reports.

IGMP report suppression is enabled by default. When it is enabled, the switch forwards only one IGMP report per multicast router query. When report suppression is disabled, all IGMP reports are forwarded to the multicast routers.

Beginning in privileged EXEC mode, follow these steps to disable IGMP report suppression:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>no ip igmp snooping report-suppression</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
</tr>
<tr>
<td>Step 4</td>
<td>show ip igmp snooping</td>
</tr>
<tr>
<td>Step 5</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To re-enable IGMP report suppression, use the `ip igmp snooping report-suppression` global configuration command.

Displaying IGMP Snooping Information

You can display IGMP snooping information for dynamically learned and statically configured router ports and VLAN interfaces. You can also display MAC address multicast entries for a VLAN configured for IGMP snooping.

To display IGMP snooping information, use one or more of the privileged EXEC commands in Table 23-4.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip igmp snooping [vlan vlan-id]</td>
<td>Display the snooping configuration information for all VLANs on the switch or for a specified VLAN. (Optional) Enter <code>vlan vlan-id</code> to display information for a single VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094.</td>
</tr>
</tbody>
</table>
| show ip igmp snooping groups [count | dynamic [count] | user [count]] | Display multicast table information for the switch or about a specific parameter:  
  - `count`—Display the total number of entries for the specified command options instead of the actual entries.  
  - `dynamic`—Display entries learned through IGMP snooping.  
  - `user`—Display only the user-configured multicast entries. |
Table 23-4 Commands for Displaying IGMP Snooping Information (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`show ip igmp snooping groups vlan [vlan-id</td>
<td>Display multicast table information for a multicast VLAN or about a specific parameter for the VLAN:</td>
</tr>
<tr>
<td>`ip_address</td>
<td>count]</td>
</tr>
<tr>
<td></td>
<td>• <code>vlan-id</code>—The VLAN ID range is 1 to 1001 and 1006 to 4094.</td>
</tr>
<tr>
<td></td>
<td>• <code>count</code>—Display the total number of entries for the specified command options instead of the actual entries.</td>
</tr>
<tr>
<td></td>
<td>• <code>dynamic</code>—Display entries learned through IGMP snooping.</td>
</tr>
<tr>
<td></td>
<td>• <code>ip_address</code>—Display characteristics of the multicast group with the specified group IP address.</td>
</tr>
<tr>
<td></td>
<td>• <code>user</code>—Display only the user-configured multicast entries.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`show ip igmp snooping mrouter [vlan vlan-id]</td>
<td>Display information on dynamically learned and manually configured multicast router interfaces.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> When you enable IGMP snooping, the switch automatically learns the interface to which a multicast router is connected. These are dynamically learned interfaces.</td>
</tr>
<tr>
<td></td>
<td><em>(Optional)</em> Enter <code>vlan vlan-id</code> to display information for a single VLAN.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`show ip igmp snooping querier [vlan vlan-id]</td>
<td>Display information about the IP address and incoming port for the most-recently received IGMP query messages in the VLAN.</td>
</tr>
<tr>
<td></td>
<td><em>(Optional)</em> Enter <code>vlan vlan-id</code> to display information for a single VLAN.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`show ip igmp snooping querier [vlan vlan-id] detail</td>
<td>Display information about the IP address and incoming port of the most-recently received IGMP query message in the VLAN and the configuration and operational state of the IGMP snooping querier in the VLAN.</td>
</tr>
</tbody>
</table>

For more information about the keywords and options in these commands, see the command reference for this release.

**Understanding Multicast VLAN Registration**

Multicast VLAN Registration (MVR) is designed for applications using wide-scale deployment of multicast traffic across an Ethernet ring-based service provider network (for example, the broadcast of multiple television channels over a service-provider network). MVR allows a subscriber on a port to subscribe and unsubscribe to a multicast stream on the network-wide multicast VLAN. It allows the single multicast VLAN to be shared in the network while subscribers remain in separate VLANs. MVR provides the ability to continuously send multicast streams in the multicast VLAN, but to isolate the streams from the subscriber VLANs for bandwidth and security reasons.

MVR assumes that subscriber ports subscribe and unsubscribe (join and leave) these multicast streams by sending out IGMP join and leave messages. These messages can originate from an IGMP Version-2-compatible host with an Ethernet connection. Although MVR operates on the underlying mechanism of IGMP snooping, the two features operate independently of each other. One can be enabled or disabled without affecting the behavior of the other feature. However, if IGMP snooping and MVR are both enabled, MVR reacts only to join and leave messages from multicast groups configured under MVR. Join and leave messages from all other multicast groups are managed by IGMP snooping.
Understanding Multicast VLAN Registration

The switch CPU identifies the MVR IP multicast streams and their associated IP multicast group in the switch forwarding table, intercepts the IGMP messages, and modifies the forwarding table to include or remove the subscriber as a receiver of the multicast stream, even though the receivers might be in a different VLAN from the source. This forwarding behavior selectively allows traffic to cross between different VLANs.

You can set the switch for compatible or dynamic mode of MVR operation.

- In compatible mode, multicast data received by MVR hosts is forwarded to all MVR data ports, regardless of MVR host membership on those ports. The multicast data is forwarded only to those receiver ports which MVR hosts have explicitly joined, either by IGMP reports or by MVR static configuration. Also, IGMP reports received from MVR hosts are never forwarded out of MVR data ports that were configured in the switch.

- In dynamic mode, multicast data received by MVR hosts on the switch is forwarded from only those MVR data and client ports that the MVR hosts have explicitly joined, either by IGMP reports or by MVR static configuration. Any IGMP reports received from MVR hosts are also forwarded from all the MVR data ports in the switch. This eliminates using unnecessary bandwidth on MVR data port links, which occurs when the switch runs in compatible mode.

Only Layer 2 ports take part in MVR. You must configure ports as MVR receiver ports. Only one MVR multicast VLAN per switch is supported.

Using MVR in a Multicast Television Application

In a multicast television application, a PC or a television with a set-top box can receive the multicast stream. Multiple set-top boxes or PCs can be connected to one subscriber port, which is a switch port configured as an MVR receiver port. Figure 23-3 is an example configuration. DHCP assigns an IP address to the set-top box or the PC. When a subscriber selects a channel, the set-top box or PC sends an IGMP report to Switch A to join the appropriate multicast. If the IGMP report matches one of the configured IP multicast group addresses, the switch CPU modifies the hardware address table to include this receiver port and VLAN as a forwarding destination of the specified multicast stream when it is received from the multicast VLAN. Uplink ports that send and receive multicast data to and from the multicast VLAN are called MVR source ports.
When a subscriber changes channels or turns off the television, the set-top box sends an IGMP leave message for the multicast stream. The switch CPU sends a MAC-based general query through the receiver port VLAN. If there is another set-top box in the VLAN still subscribing to this group, that set-top box must respond within the maximum response time specified in the query. If the CPU does not receive a response, it eliminates the receiver port as a forwarding destination for this group.

Without Immediate Leave, when the switch receives an IGMP leave message from a subscriber on a receiver port, it sends out an IGMP query on that port and waits for IGMP group membership reports. If no reports are received in a configured time period, the receiver port is removed from multicast group membership. With Immediate Leave, an IGMP query is not sent from the receiver port on which the IGMP leave was received. As soon as the leave message is received, the receiver port is removed from multicast group membership, which speeds up leave latency. Enable the Immediate Leave feature only on receiver ports to which a single receiver device is connected.

MVR eliminates the need to duplicate television-channel multicast traffic for subscribers in each VLAN. Multicast traffic for all channels is only sent around the VLAN trunk once—only on the multicast VLAN. The IGMP leave and join messages are in the VLAN to which the subscriber port is assigned. These messages dynamically register for streams of multicast traffic in the multicast VLAN on the
Layer 3 device. The access layer switch (Switch A) modifies the forwarding behavior to allow the traffic to be forwarded from the multicast VLAN to the subscriber port in a different VLAN, selectively allowing traffic to cross between two VLANs.

IGMP reports are sent to the same IP multicast group address as the multicast data. The Switch A CPU must capture all IGMP join and leave messages from receiver ports and forward them to the multicast VLAN of the source (uplink) port, based on the MVR mode.

Configuring MVR

These sections include basic MVR configuration information:

- Default MVR Configuration, page 23-16
- MVR Configuration Guidelines and Limitations, page 23-16
- Configuring MVR Global Parameters, page 23-17
- Configuring MVR on Access Ports, page 23-18
- Configuring MVR on Trunk Ports, page 23-20
- Displaying MVR Information, page 23-21

Default MVR Configuration

Table 23-5 shows the default MVR configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>MVR</td>
<td>Disabled globally and per interface</td>
</tr>
<tr>
<td>Multicast addresses</td>
<td>None configured</td>
</tr>
<tr>
<td>Query response time</td>
<td>0.5 second</td>
</tr>
<tr>
<td>Multicast VLAN</td>
<td>VLAN 1</td>
</tr>
<tr>
<td>Mode</td>
<td>Compatible</td>
</tr>
<tr>
<td>Interface (per port) default</td>
<td>Neither a receiver nor a source port</td>
</tr>
<tr>
<td>Immediate Leave</td>
<td>Disabled on all ports</td>
</tr>
</tbody>
</table>

MVR Configuration Guidelines and Limitations

Follow these guidelines when configuring MVR:

- Receiver ports on a switch can be in different VLANs, but they should not belong to the multicast VLAN.
- Trunk ports or access ports can be configured as receiver ports.
- When MVR mode is compatible (the default), you can configure only 512 MVR groups.
- When MVR mode is dynamic, the maximum number of multicast entries (MVR group addresses) that can be configured on a switch is 2000. The maximum number of simultaneous active multicast streams (that is, the maximum number of television channels that can be receiving) is 512. When
Configuring IGMP Snooping and MVR

Chapter 23

this limit is reached, a message is generated that the Maximum hardware limit of groups had been reached. Note that a hardware entry occurs when there is an IGMP join on a port or when you have configured the port to join a group by entering the `mvr vlan vlan-id group ip-address` interface configuration command.

- MVR multicast data received in the source VLAN and leaving from receiver ports has its time-to-live (TTL) decremented by 1 in the switch.
- Because MVR on the switch uses IP multicast addresses instead of MAC multicast addresses, aliased IP multicast addresses are allowed on the switch. However, if the switch is interoperating with Catalyst 3550 or Catalyst 3500 XL switches, you should not configure IP addresses that alias between themselves or with the reserved IP multicast addresses (in the range 224.0.0.xxx).
- Do not configure MVR on private VLAN ports.
- MVR is not supported when multicast routing is enabled on a switch. If you enable multicast routing and a multicast routing protocol while MVR is enabled, MVR is disabled, and you receive a warning message. If you try to enable MVR while multicast routing and a multicast routing protocol are enabled, the operation to enable MVR is cancelled, and you receive an error message.
- MVR can coexist with IGMP snooping on a switch.
- MVR data received on an MVR receiver port is not forwarded to MVR source ports.
- MVR does not support IGMPv3 messages.
- Starting with Cisco IOS release 12.2(52)SE, you can enter the `mvr ringmode flood` global configuration to ensure that data forwarding in a ring topology is limited to ports detected as members and excludes forwarding to multicast router ports. This prevents unicast traffic from being dropped in a ring environment when MVR multicast traffic flows in one direction and unicast traffic flows in the other direction.

Configuring MVR Global Parameters

You do not need to set the optional MVR parameters if you choose to use the default settings. If you do want to change the default parameters (except for the MVR VLAN), you must first enable MVR.

For complete syntax and usage information for the commands used in this section, see the command reference for this release.

Beginning in privileged EXEC mode, follow these steps to configure MVR parameters:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>mvr</code></td>
<td>Enable MVR on the switch.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
</tbody>
</table>
| `mvr group ip-address [count]` | Configure an IP multicast address on the switch or use the `count` parameter to configure a contiguous series of MVR group addresses. The range for count is 1 to 2000. However, when the MVR mode is compatible, the switch allows a maximum count of 512. When the mode is dynamic, you can create 2000 MVR groups. The default is 1.

Any multicast data sent to this address is sent to all source ports on the switch and all receiver ports that have elected to receive data on that multicast address. Each multicast address would correspond to one television channel. |
### Configuring MVR

#### Step 4
**Command**: `mvr querytime value`
**Purpose**: (Optional) Define the maximum time to wait for IGMP report memberships on a receiver port before removing the port from multicast group membership. The value is in units of tenths of a second. The range is 1 to 100 and the default is 5 tenths or one-half second.

#### Step 5
**Command**: `mvr vlan vlan-id`
**Purpose**: (Optional) Specify the VLAN in which multicast data is received; all source ports must belong to this VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094. The default is VLAN 1.

#### Step 6
**Command**: `mvr mode {dynamic | compatible}`
**Purpose**: (Optional) Specify the MVR mode of operation:
- **dynamic**—Allow dynamic MVR membership on source ports. To configure 2000 MVR groups, the mode must be **dynamic**.
- **compatible**—Is compatible with Catalyst 3500 XL and Catalyst 2900 XL switches and does not support IGMP dynamic joins on source ports.

The default is **compatible** mode.

#### Step 7
**Command**: `mvr ringmode flood`
**Purpose**: (Optional) Enable MVR ringmode flooding for access rings. Entering this command controls traffic flow in egress ports in a ring environment to prevent the dropping of unicast traffic.

#### Step 8
**Command**: `end`
**Purpose**: Return to privileged EXEC mode.

#### Step 9
**Command**: `show mvr` or `show mvr members`
**Purpose**: Verify the configuration.

#### Step 10
**Command**: `copy running-config startup-config`
**Purpose**: (Optional) Save your entries in the configuration file.

To return the switch to its default settings, use the `no mvr [mode | group ip-address | querytime | vlan]` global configuration commands.

This example shows how to enable MVR, configure the group address, set the query time to 1 second (10 tenths), specify the MVR multicast VLAN as VLAN 22, and set the MVR mode as dynamic:

```
Switch(config)# mvr
Switch(config)# mvr group 228.1.23.4
Switch(config)# mvr querytime 10
Switch(config)# mvr vlan 22
Switch(config)# mvr mode dynamic
Switch(config)# end
```

You can use the `show mvr members` privileged EXEC command to verify the MVR multicast group addresses on the switch.

### Configuring MVR on Access Ports

Beginning in privileged EXEC mode, follow these steps to configure Layer 2 MVR interfaces:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> mvr</td>
<td>Enable MVR on the switch.</td>
</tr>
<tr>
<td><strong>Step 3</strong> interface interface-id</td>
<td>Enter interface configuration mode, and enter the type and number of the Layer 2 port to configure.</td>
</tr>
</tbody>
</table>
Configuring MVR

To return the interface to its default settings, use the `no mvr [type | immediate | vlan vlan-id | group]` interface configuration commands.

This example shows how to configure an interface as a receiver port, statically configure the port to receive multicast traffic sent to the multicast group address, configure Immediate Leave on the interface, and verify the results.

```
Switch(config)# mvr
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# mvr type receiver
Switch(config-if)# mvr vlan 22 group 228.1.23.4
Switch(config-if)# mvr immediate
Switch(config-if)# end
Switch# show mvr interface
Port       Type     Mode    VLAN  Status         Immediate Leave
Gia1/0/2    RECEIVER Trunk  201   ACTIVE/DOWN    DISABLED
```
Configuring MVR on Trunk Ports

In Cisco IOS Release 12.2(25)SEG and earlier, only access ports could be configured as MVR receiver ports. In Cisco IOS Release 12.2(35)SE and later, you can also configure trunk ports as MVR receiver ports.

**Note**

For more information about access and trunk ports, see Chapter 9, “Configuring Interface Characteristics”.

Beginning in privileged EXEC mode, follow these steps to configure a trunk port as an MVR receiver port:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>mvr Enable MVR on the switch.</td>
</tr>
<tr>
<td>Step 3</td>
<td>interface interface-id Enter the Layer 2 port to configure and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>switchport mode trunk Set trunking mode to TRUNK unconditionally.</td>
</tr>
<tr>
<td>Step 5</td>
<td>mvr type receiver Specify that the trunk port is an MVR receiver port.</td>
</tr>
<tr>
<td>Step 6</td>
<td>mvr vlan source-vlan-id receiver vlan receiver-vlan-id Enable this trunk port to distribute MVR traffic coming from the MVR VLAN to the VLAN on the trunk identified by the receiver VLAN.</td>
</tr>
<tr>
<td>Step 7</td>
<td>mvr vlan vlan-id group ip-address receiver vlan-id (Optional) Configure the trunk port to be a static member of the group on the receiver VLAN.</td>
</tr>
<tr>
<td>Step 8</td>
<td>end Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 9</td>
<td>show mvr Verify the configuration.</td>
</tr>
<tr>
<td>show mvr interface</td>
<td></td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td>show mvr members</td>
<td></td>
</tr>
<tr>
<td>Step 10</td>
<td>copy running-config startup-config (Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

This example shows how to configure a port as an MVR trunk receiver port, assign it to a VLAN, configure the port to be a static member of a group, and verify the results.

```
Switch(config)# mvr
Switch(config)# interface fastethernet 0/10
Switch(config)# switchport mode trunk
Switch(config)# mvr type receiver
Switch(config)# mvr vlan 100 receiver vlan 201
Switch(config)# mvr vlan 100 group 239.1.1.1 receiver vlan 201
Switch(config)# end
Switch# show mvr interface
```

To return the interface to its default settings, use the `no mvr [type | immediate | vlan vlan-id | group]` interface configuration command.
Displaying MVR Information

You can display MVR information for the switch or for a specified interface. Beginning in privileged EXEC mode, use the commands in Table 23-6 to display MVR configuration:

<table>
<thead>
<tr>
<th>Table 23-6</th>
<th>Commands for Displaying MVR Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>show mvr</strong></td>
<td>Displays MVR status and values for the switch—whether MVR is enabled or disabled, the multicast VLAN, the maximum (512) and current (0 through 512) number of multicast groups, the query response time, and the MVR mode.</td>
</tr>
</tbody>
</table>
| **show mvr interface** [interface-id] [members [vlan vlan-id]] | Displays all MVR interfaces and their MVR configurations. When a specific interface is entered, displays this information:  
  - Type—Receiver or Source  
  - Mode—Access or Trunk  
  - VLAN—The MVR VLAN for the source port and the receiver VLAN for the receiver port  
  - Status—One of these:  
    - Active means the port is part of a VLAN.  
    - Up/Down means that the port is forwarding or nonforwarding.  
    - Inactive means that the port is not part of any VLAN.  
  - Immediate Leave—Enabled or Disabled  
When the **members** keyword is entered, displays all multicast group members on this port or, if a VLAN identification is entered, all multicast group members on the VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094. |
| **show mvr members** [ip-address] | Displays all receiver and source ports that are members of any IP multicast group or the specified IP multicast group IP address. |

Configuring IGMP Filtering and Throttling

In some environments, for example, metropolitan or multiple-dwelling unit (MDU) installations, you might want to control the set of multicast groups to which a user on a switch port can belong. You can control the distribution of multicast services, such as IP/TV, based on some type of subscription or service plan. You might also want to limit the number of multicast groups to which a user on a switch port can belong.

With the IGMP filtering feature, you can filter multicast joins on a per-port basis by configuring IP multicast profiles and associating them with individual switch ports. An IGMP profile can contain one or more multicast groups and specifies whether access to the group is permitted or denied. If an IGMP profile denying access to a multicast group is applied to a switch port, the IGMP join report requesting the stream of IP multicast traffic is dropped, and the port is not allowed to receive IP multicast traffic from that group. If the filtering action permits access to the multicast group, the IGMP report from the port is forwarded for normal processing.

IGMP filtering controls only group specific query and membership reports, including join and leave reports. It does not control general IGMP queries. IGMP filtering has no relationship with the function that directs the forwarding of IP multicast traffic. The filtering feature operates in the same manner whether CGMP or MVR is used to forward the multicast traffic.
IGMP filtering is only applicable to dynamic learning of IP multicast group addresses; not static configuration.

With the IGMP throttling feature, you can also set the maximum number of IGMP groups that a Layer 2 interface can join. If the maximum number of IGMP groups is set, the IGMP snooping forwarding table contains the maximum number of entries, and the interface receives an IGMP join report, you can configure an interface to drop the IGMP report or to replace the randomly selected multicast entry with the received IGMP report.

Note

IGMPv3 join and leave messages are not supported on switches running IGMP filtering.

These sections describe how to configure IGMP filtering and throttling:

- Default IGMP Filtering and Throttling Configuration, page 23-22
- Configuring IGMP Profiles, page 23-22 (optional)
- Applying IGMP Profiles, page 23-23 (optional)
- Setting the Maximum Number of IGMP Groups, page 23-24 (optional)
- Configuring the IGMP Throttling Action, page 23-25 (optional)

**Default IGMP Filtering and Throttling Configuration**

Table 23-7 shows the default IGMP filtering configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP filters</td>
<td>None applied</td>
</tr>
<tr>
<td>IGMP Maximum number of IGMP groups</td>
<td>No maximum set</td>
</tr>
<tr>
<td>IGMP profiles</td>
<td>None defined</td>
</tr>
<tr>
<td>IGMP profile action</td>
<td>Deny the range addresses</td>
</tr>
</tbody>
</table>

When the maximum number of groups is in forwarding table, the default IGMP throttling action is to deny the IGMP report. For configuration guidelines, see the Configuring the IGMP Throttling Action, page 23-25.

**Configuring IGMP Profiles**

To configure an IGMP profile, use the `ip igmp profile` global configuration command with a profile number to create an IGMP profile and to enter IGMP profile configuration mode. From this mode, you can specify the parameters of the IGMP profile to be used for filtering IGMP join requests from a port. When you are in IGMP profile configuration mode, you can create the profile by using these commands:

- **deny**: Specifies that matching addresses are denied; this is the default condition.
- **exit**: Exits from igmp-profile configuration mode.
- **no**: Negates a command or sets its defaults.
- **permit**: Specifies that matching addresses are permitted.
Chapter 23 Configuring IGMP Snooping and MVR

Configuring IGMP Filtering and Throttling

- **range**: Specifies a range of IP addresses for the profile. You can enter a single IP address or a range with a start and an end address.

The default is for the switch to have no IGMP profiles configured. When a profile is configured, if neither the **permit** nor **deny** keyword is included, the default is to deny access to the range of IP addresses.

Beginning in privileged EXEC mode, follow these steps to create an IGMP profile:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>ip igmp profile profile number</code></td>
<td>Enter IGMP profile configuration mode, and assign a number to the profile you are configuring. The range is 1 to 4294967295.</td>
</tr>
<tr>
<td>Step 3</td>
<td>`permit</td>
<td>deny`</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>range ip multicast address</code></td>
<td>Enter the IP multicast address or range of IP multicast addresses to which access is being controlled. If entering a range, enter the low IP multicast address, a space, and the high IP multicast address. You can use the <code>range</code> command multiple times to enter multiple addresses or ranges of addresses.</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 6</td>
<td><code>show ip igmp profile profile number</code></td>
<td>Verify the profile configuration.</td>
</tr>
<tr>
<td>Step 7</td>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To delete a profile, use the **no ip igmp profile profile number** global configuration command.

To delete an IP multicast address or range of IP multicast addresses, use the **no range ip multicast address** IGMP profile configuration command.

This example shows how to create IGMP profile 4 allowing access to the single IP multicast address and how to verify the configuration. If the action was to deny (the default), it would not appear in the `show ip igmp profile` output display.

```
Switch(config)# ip igmp profile 4
Switch(config-igmp-profile)# permit
Switch(config-igmp-profile)# range 229.9.9.0
Switch(config-igmp-profile)# end
Switch# show ip igmp profile 4
IGMP Profile 4
  permit
  range 229.9.9.0 229.9.9.0
```

**Applying IGMP Profiles**

To control access as defined in an IGMP profile, use the **ip igmp filter** interface configuration command to apply the profile to the appropriate interfaces. You can apply IGMP profiles to layer 2 access ports only; you cannot apply IGMP profiles to routed ports or SVIs. You cannot apply profiles to ports that belong to an EtherChannel port group. You can apply a profile to multiple interfaces, but each interface can only have one profile applied to it.
Beginning in privileged EXEC mode, follow these steps to apply an IGMP profile to a switch port:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Enter interface configuration mode, and enter the physical interface to configure. The interface must be a Layer 2 port that does not belong to an EtherChannel port group.</td>
</tr>
<tr>
<td>Step 3 ip igmp filter profile number</td>
<td>Apply the specified IGMP profile to the interface. The profile number can be from 1 to 4294967295.</td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5 show running-config interface interface-id</td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td>Step 6 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To remove a profile from an interface, use the **no ip igmp filter profile number** interface configuration command.

This example shows how to apply IGMP profile 4 to a port:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip igmp filter 4
Switch(config-if)# end
```

### Setting the Maximum Number of IGMP Groups

You can set the maximum number of IGMP groups that a Layer 2 interface can join by using the **ip igmp mac-groups number** interface configuration command. Use the **no** form of this command to set the maximum back to the default, which is no limit.

This restriction can be applied to Layer 2 ports only; you cannot set a maximum number of IGMP groups on routed ports or SVIs. You also cannot use this command on ports that belong to an EtherChannel port group.

Beginning in privileged EXEC mode, follow these steps to apply an IGMP profile to a switch port:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Enter interface configuration mode, and enter the physical interface to configure. The interface must be a Layer 2 port that does not belong to an EtherChannel group.</td>
</tr>
<tr>
<td>Step 3 ip igmp max-groups number</td>
<td>Set the maximum number of IGMP groups that the interface can join. The range is 0 to 4294967294. The default is to have no maximum set.</td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5 show running-config interface interface-id</td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td>Step 6 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
To remove the maximum group limitation and return to the default of no maximum, use the `no ip igmp max-groups` interface configuration command.

This example shows how to limit the number of IGMP groups that a port can join to 25.

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip igmp max-groups 25
Switch(config-if)# end
```

## Configuring the IGMP Throttling Action

After you set the maximum number of IGMP groups that a Layer 2 interface can join, you can configure an interface to replace the existing group with the new group for which the IGMP report was received by using the `ip igmp max-groups action replace` interface configuration command. Use the `no` form of this command to return to the default, which is to drop the IGMP join report.

Follow these guidelines when configuring the IGMP throttling action:

- This restriction can be applied only to Layer 2 ports. You can use this command on a logical EtherChannel interface but cannot use it on ports that belong to an EtherChannel port group.
- When the maximum group limitation is set to the default (no maximum), entering the `ip igmp max-groups action {deny | replace}` command has no effect.
- If you configure the throttling action and set the maximum group limitation after an interface has added multicast entries to the forwarding table, the forwarding-table entries are either aged out or removed, depending on the throttling action:
  - If you configure the throttling action as `deny`, the entries that were previously in the forwarding table are not removed but are aged out. After these entries are aged out and the maximum number of entries is in the forwarding table, the switch drops the next IGMP report received on the interface.
  - If you configure the throttling action as `replace`, the entries that were previously in the forwarding table are removed. When the maximum number of entries is in the forwarding table, the switch replaces a randomly selected entry with the received IGMP report.

To prevent the switch from removing the forwarding-table entries, you can configure the IGMP throttling action before an interface adds entries to the forwarding table.

Beginning in privileged EXEC mode, follow these steps to configure the throttling action when the maximum number of entries is in the forwarding table:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td><code>interface interface-id</code></td>
<td>Enter interface configuration mode, and enter the physical interface to configure. The interface can be a Layer 2 port that does not belong to an EtherChannel group or an EtherChannel interface. The interface cannot be a trunk port.</td>
</tr>
</tbody>
</table>
| 3    | `ip igmp max-groups action {deny | replace}` | When an interface receives an IGMP report and the maximum number of entries is in the forwarding table, specify the action that the interface takes:  
  - `deny`—Drop the report.
  - `replace`—Replace the existing group for which the IGMP report was received. |
Chapter 23  Configuring IGMP Snooping and MVR

Displaying IGMP Snooping and MVR

Displaying IGMP Filtering and Throttling Configuration

To return to the default action of dropping the report, use the **no ip igmp max-groups action** interface configuration command.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4  end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5  show running-config</td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td>interface</td>
<td></td>
</tr>
<tr>
<td>interface-id</td>
<td></td>
</tr>
<tr>
<td>Step 6  copy running-config</td>
<td>(Optional) Save your entries in the configuration</td>
</tr>
<tr>
<td>startup-config</td>
<td>file.</td>
</tr>
</tbody>
</table>

To return to the default action of dropping the report, use the **no ip igmp max-groups action** interface configuration command.

**Displaying IGMP Filtering and Throttling Configuration**

You can display IGMP profile characteristics, and you can display the IGMP profile and maximum group configuration for all interfaces on the switch or for a specified interface. You can also display the IGMP throttling configuration for all interfaces on the switch or for a specified interface.

Use the privileged EXEC commands in Table 23-8 to display IGMP filtering and throttling configuration:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip igmp profile [profile</td>
<td>Displays the specified IGMP profile or all IGMP</td>
</tr>
<tr>
<td>number]</td>
<td>profiles defined on the switch.</td>
</tr>
<tr>
<td>show running-config [interface</td>
<td>Displays the configuration of the specified</td>
</tr>
<tr>
<td>interface-id]</td>
<td>interface or the configuration of all interfaces</td>
</tr>
<tr>
<td></td>
<td>on the switch, including (if configured) the</td>
</tr>
<tr>
<td></td>
<td>maximum number of IGMP groups to which an</td>
</tr>
<tr>
<td></td>
<td>interface can belong and the IGMP profile</td>
</tr>
<tr>
<td></td>
<td>applied to the interface.</td>
</tr>
</tbody>
</table>
CHAPTER 24

Configuring Port-Based Traffic Control

This chapter describes how to configure port-based traffic control features on the Catalyst 3750 Metro switch.

For complete syntax and usage information for the commands used in this chapter, see the command reference for this release.

This chapter consists of these sections:
- Configuring Storm Control, page 24-1
- Configuring Protected Ports, page 24-6
- Configuring Port Blocking, page 24-7
- Configuring Port Security, page 24-8

Configuring Storm Control

These sections include storm control configuration information and procedures:
- Understanding Storm Control, page 24-1
- Default Storm Control Configuration, page 24-3
- Configuring Storm Control and Threshold Levels, page 24-3
- Configuring Small-Frame Arrival Rate, page 24-5

Understanding Storm Control

Storm control prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on one of the physical interfaces. A LAN storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. Errors in the protocol-stack implementation, mistakes in the network configuration, and users issuing a denial-of-service attack can cause a storm.

Storm control uses one of these methods to measure traffic activity:
- Bandwidth as a percentage of the total available bandwidth of the port that can be used by the broadcast, multicast, or unicast traffic
- Traffic rate in packets per second at which broadcast, multicast, or unicast packets are received (Cisco IOS Release 12.2(25)EY or later)
• Traffic rate in bits per second at which broadcast, multicast, or unicast packets are received (Cisco IOS Release 12.2(25)EY or later)
• Traffic rate in packets per second and for small frames. This feature is enabled globally. The threshold for small frames is configured for each interface. (Cisco IOS Release 12.2(44)SE or later)

With each method, the port blocks traffic when the rising threshold is reached. The port remains blocked until the traffic rate drops below the falling threshold (if one is specified) and then resumes normal forwarding. If the falling suppression level is not specified, the switch blocks all traffic until the traffic rate drops below the rising suppression level. In general, the higher the level, the less effective the protection against broadcast storms.

**Note**

When the storm control threshold for multicast traffic is reached, all multicast traffic except control traffic, such as bridge protocol data unit (BDPU) and Cisco Discovery Protocol (CDP) frames, are blocked. However, the switch does not differentiate between routing updates, such as OSPF, and regular multicast data traffic, so both types of traffic are blocked.

When storm control is enabled, the switch monitors packets passing from an interface to the switching bus and determines if the packet is unicast, multicast, or broadcast. The switch monitors the number of broadcast, multicast, or unicast packets received within a 200-millisecond time interval, and when a threshold for one type of traffic is reached, that type of traffic is dropped. This threshold is specified as a percentage of total available bandwidth that can be used by broadcast (multicast or unicast) traffic.

The graph in Figure 24-1 shows broadcast traffic patterns on an interface over a given period of time. The example can also be applied to multicast and unicast traffic. In this example, the broadcast traffic being forwarded exceeded the configured threshold between time intervals T1 and T2 and between T4 and T5. When the amount of specified traffic exceeds the threshold, all traffic of that kind is dropped for the next time period. Therefore, broadcast traffic is blocked during the intervals following T2 and T5. At the next time interval (for example, T3), if broadcast traffic does not exceed the threshold, it is again forwarded.

**Figure 24-1 Broadcast Storm Control Example**

The combination of the storm-control suppression level and the 200-millisecond time interval control the way the storm control algorithm works. A higher threshold allows more packets to pass through. A threshold value of 100 percent means that no limit is placed on the traffic. A value of 0.0 means that all broadcast, multicast, or unicast traffic on that port is blocked.
Because packets do not arrive at uniform intervals, the 200-millisecond time interval during which traffic activity is measured can affect the behavior of storm control.

The switch continues to monitor traffic on the port, and when the utilization level is below the threshold level, the type of traffic that was dropped is forwarded again.

You use the `storm-control` interface configuration commands to set the threshold value for each traffic type.

**Default Storm Control Configuration**

By default, unicast, broadcast, and multicast storm control is disabled on the switch interfaces; that is, the suppression level is 100 percent.

**Configuring Storm Control and Threshold Levels**

You configure storm control on a port and enter the threshold level that you want to be used for a particular type of traffic.

However, because of hardware limitations and the way in which packets of different sizes are counted, threshold percentages are approximations. Depending on the sizes of the packets making up the incoming traffic, the actual enforced threshold might differ from the configured level by several percentage points.

Follow these guidelines when configuring storm control:

- If the switch is acting as a label switch router (LSR), multiprotocol label switching (MPLS) traffic between two enhanced-services (ES) ports is not counted.
- If an ingress hierarchical quality-of-service (QoS) service policy is attached to an ES port, the actions specified in the service policy are processed before storm control takes affect. The switch might be receiving traffic at a higher rate than the configured thresholds, but actions in the service policy might reduce the rate at which traffic is received, preventing storm-control actions from occurring.

**Note** Storm control is supported on physical interfaces. You can also configure storm control on an EtherChannel. When storm control is configured on an EtherChannel, the storm control settings propagate to the EtherChannel physical interfaces.

Beginning in privileged EXEC mode, follow these steps to enable a particular type of storm control:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><code>interface interface-id</code></td>
<td>Enter interface configuration mode, and enter the type and number of the physical interface to configure, for example <code>gigabitethernet1/0/1</code>.</td>
</tr>
</tbody>
</table>
### Configuring Storm Control

#### Step 3

**Command**
```
storm-control { broadcast | multicast | unicast } level { level [level-low] | bps bps [bps-low] | pps pps [pps-low] }
```

**Purpose**
Configure broadcast, multicast, or unicast storm control. By default, storm control is disabled.

The keywords have these meanings:

- For **level**, specify the rising threshold level for broadcast, multicast, or unicast traffic as a percentage (up to two decimal places) of the bandwidth. The port blocks traffic when the rising threshold is reached. The range is **0.00 to 100.00**.

- (Optional) For **level-low**, specify the falling threshold level as a percentage (up to two decimal places) of the bandwidth. This **value must be less than or equal to the rising suppression value**. The port forwards traffic when traffic drops below this level. If you do not configure a falling suppression level, it is set to the rising suppression level. The range is **0.00 to 100.00**.

If you set the threshold to the maximum value (100 percent), no limit is placed on the traffic. If you set the threshold to 0.0, all broadcast, multicast, and unicast traffic on that port is blocked.

- For **bps bps**, specify the rising threshold level for broadcast, multicast, or unicast traffic in bits per second (up to one decimal place). The port blocks traffic when the rising threshold is reached. The range is **0.0 to 10000000000.0**.

- (Optional) For **bps-low**, specify the falling threshold level in bits per second (up to one decimal place). It can be less than or equal to the rising threshold level. The port forwards traffic when traffic drops below this level. The range is **0.0 to 10000000000.0**.

- For **pps pps**, specify the rising threshold level for broadcast, multicast, or unicast traffic in packets per second (up to one decimal place). The port blocks traffic when the rising threshold is reached. The range is **0.0 to 10000000000.0**.

- (Optional) For **pps-low**, specify the falling threshold level in packets per second (up to one decimal place). It can be less than or equal to the rising threshold level. The port forwards traffic when traffic drops below this level. The range is **0.0 to 10000000000.0**.

For BPS and PPS settings, you can use metric suffixes such as k, m, and g for large number thresholds.

#### Step 4

**Command**
```
storm-control action { shutdown | trap }
```

**Purpose**
Specify the action to be taken when a storm is detected. The default is to filter out the traffic and not to send traps.

- Select the **shutdown** keyword to error-disable the port during a storm.
- Select the **trap** keyword to generate an SNMP trap when a storm is detected.

#### Step 5

**Command**
```
end
```

**Purpose**
Return to privileged EXEC mode.
To disable storm control, use the `no storm-control {broadcast | multicast | unicast} level` interface configuration command.

This example shows how to enable unicast storm control on a port with an 87-percent rising suppression level and a 65-percent falling suppression level:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# storm-control unicast level 87 65
```

This example shows how to enable broadcast address storm control on a port to a level of 20 percent. When the broadcast traffic exceeds the configured level of 20 percent of the total available bandwidth of the port within the traffic-storm-control interval, the switch drops all broadcast traffic until the end of the traffic-storm-control interval:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# storm-control broadcast level 20
```

## Configuring Small-Frame Arrival Rate

Incoming VLAN-tagged packets smaller than 67 bytes are considered small frames. They are forwarded by the switch, but they do not cause the switch storm-control counters to increment. In Cisco IOS Release 12.2(44)SE and later, you can configure a port to be error disabled if small frames arrive at a specified rate (threshold).

You globally enable the small-frame rate-arrival feature on the switch and then configure the small-frame threshold for packets on each interface. Packets smaller than the minimum size and arriving at a specified rate (the threshold) are dropped since the port is error disabled.

If the `errdisable recovery cause small-frame` global configuration command is entered, the port is re-enabled after a specified time. (You specify the recovery time by using `errdisable recovery` global configuration command.)

Beginning in privileged EXEC mode, follow these steps to configure the threshold level for each interface:

### Configuring Small-Frame Arrival Rate

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>errdisable detect cause small-frame</td>
<td>Enable the small-frame rate-arrival feature on the switch.</td>
</tr>
<tr>
<td><code>errdisable recovery interval interval</code></td>
<td>(Optional) Specify the time to recover from the specified error-disabled state.</td>
</tr>
<tr>
<td>errdisable recovery cause small-frame</td>
<td>(Optional) Configure the recovery time for error-disabled ports to be automatically re-enabled after they are error disabled by the arrival of small frames</td>
</tr>
</tbody>
</table>
### Configuring Protected Ports

Some applications require that no traffic be forwarded at Layer 2 between ports on the same switch so that one neighbor does not see the traffic generated by another neighbor. In such an environment, the use of protected ports ensures that there is no exchange of unicast, broadcast, or multicast traffic between these ports on the switch.

Protected ports have these features:

- A protected port does not forward any traffic (unicast, multicast, or broadcast) to any other port that is also a protected port. Traffic cannot be forwarded between protected ports at Layer 2; all traffic passing between protected ports must be forwarded through a Layer 3 device.
- Forwarding behavior between a protected port and a nonprotected port proceeds as usual.

### Default Protected Port Configuration

The default is to have no protected ports defined.

### Protected Port Configuration Guidelines

You can configure protected ports on a physical interface (for example, Gigabit Ethernet1/0/1) or an EtherChannel group (for example, port-channel 5). When you enable protected ports for a port channel, it is enabled for all ports in the port-channel group.

Do not configure a private-VLAN port as a protected port. Do not configure a protected port as a private-VLAN port. A private-VLAN isolated port does not forward traffic to other isolated ports or community ports. For more information about private VLANs, see Chapter 13, “Configuring Private VLANs.”

---

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 5</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 6</td>
<td>small violation-rate pps</td>
</tr>
<tr>
<td>Step 7</td>
<td>end</td>
</tr>
<tr>
<td>Step 8</td>
<td>show interfaces interface-id</td>
</tr>
<tr>
<td>Step 9</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

This example shows how to enable the small-frame arrival-rate feature, configure the port recovery time, and configure the threshold for error disabling a port:

```
Switch# configure terminal
Switch# errdisable detect cause small-frame
Switch# errdisable recovery cause small-frame
Switch(config)# interface fastethernet0/1
Switch(config-if)# small-frame violation rate 10000
Switch(config-if)# end
```
Configuring a Protected Port

Beginning in privileged EXEC mode, follow these steps to define a port as a protected port:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Enter interface configuration mode, and enter the type and</td>
</tr>
<tr>
<td></td>
<td>number of the interface to configure, for example</td>
</tr>
<tr>
<td></td>
<td>gigabitethernet1/0/1.</td>
</tr>
<tr>
<td>Step 3 switchport protected</td>
<td>Configure the interface to be a protected port.</td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5 show interfaces interface-id switchport</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 6 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable protected port, use the no switchport protected interface configuration command.

This example shows how to configure an interface as a protected port:

```plaintext
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# switchport protected
Switch(config-if)# end
```

Configuring Port Blocking

By default, the switch floods packets with unknown destination MAC addresses out of all ports. If unknown unicast and multicast traffic is forwarded to a protected port, there could be security issues. To prevent unknown unicast or multicast traffic from being forwarded from one port to another, you can block a port (protected or nonprotected) from flooding unknown unicast or multicast packets to other ports.

**Note**

With multicast traffic, the port blocking feature blocks only pure Layer 2 packets. Multicast packets that contain IPv4 or IPv6 information in the header are not blocked.

Default Port Blocking Configuration

The default is to not block flooding of unknown multicast and unicast traffic out of a port, but to flood these packets to all ports.
Blocking Flooded Traffic on an Interface

**Note**
The interface can be a physical interface (for example, Gigabit Ethernet 1/0/1) or an EtherChannel group (for example, port-channel 5). When you block multicast or unicast traffic for a port channel, it is blocked on all ports in the port channel group.

Beginning in privileged EXEC mode, follow these steps to disable the flooding of unicast packets and Layer 2 multicast packets out of an interface:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>switchport block multicast</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>switchport block unicast</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>show interfaces interface-id switchport</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To return the interface to the default condition where no traffic is blocked and normal forwarding occurs on the port, use the `no switchport block {multicast | unicast}` interface configuration commands.

This example shows how to block unicast and Layer 2 multicast flooding on an interface:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# switchport block multicast
Switch(config-if)# switchport block unicast
Switch(config-if)# end
```

Configuring Port Security

You can use the port security feature to restrict input to an interface by limiting and identifying MAC addresses of the stations allowed to access the port. When you assign secure MAC addresses to a secure port, the port does not forward packets with source addresses outside the group of defined addresses. If you limit the number of secure MAC addresses to one and assign a single secure MAC address, the workstation attached to that port is assured the full bandwidth of the port.

If a port is configured as a secure port and the maximum number of secure MAC addresses is reached, when the MAC address of a station attempting to access the port is different from any of the identified secure MAC addresses, a security violation occurs. Also, if a station with a secure MAC address configured or learned on one secure port attempts to access another secure port, a violation is flagged.
These sections include port security configuration information and procedures:

- Understanding Port Security, page 24-9
- Default Port Security Configuration, page 24-11
- Configuration Guidelines, page 24-11
- Enabling and Configuring Port Security, page 24-12
- Enabling and Configuring Port Security Aging, page 24-15
- Port Security and Private VLANs, page 24-16

### Understanding Port Security

This section contains information about these topics:

- Secure MAC Addresses, page 24-9
- Security Violations, page 24-10

### Secure MAC Addresses

You configure the maximum number of secure addresses allowed on a port by using the `switchport port-security maximum value` interface configuration command.

**Note**

If you try to set the maximum value to a number less than the number of secure addresses already configured on an interface, the command is rejected.

The switch supports these types of secure MAC addresses:

- Static secure MAC addresses—These are manually configured by using the `switchport port-security mac-address mac-address` interface configuration command, stored in the address table, and added to the switch running configuration.
- Dynamic secure MAC addresses—These are dynamically configured, stored only in the address table, and removed when the switch restarts.
- *Sticky* secure MAC addresses—These can be dynamically learned or manually configured, stored in the address table, and added to the running configuration. If these addresses are saved in the configuration file, when the switch restarts, the interface does not need to dynamically reconfigure them.

You can configure an interface to convert the dynamic MAC addresses to sticky secure MAC addresses and to add them to the running configuration by enabling *sticky learning*. To enable sticky learning, enter the `switchport port-security mac-address sticky` interface configuration command. When you enter this command, the interface converts all the dynamic secure MAC addresses, including those that were dynamically learned before sticky learning was enabled, to sticky secure MAC addresses. All sticky secure MAC addresses are added to the running configuration.

The sticky secure MAC addresses do not automatically become part of the configuration file, which is the startup configuration used each time the switch restarts. If you save the sticky secure MAC addresses in the configuration file, when the switch restarts, the interface does not need to relearn these addresses. If you do not save the sticky secure addresses, they are lost.

If sticky learning is disabled, the sticky secure MAC addresses are converted to dynamic secure addresses and are removed from the running configuration.
The maximum number of secure MAC addresses that you can configure on a switch is determined by the maximum number of available MAC addresses allowed in the system. This number is determined by the active Switch Database Management (SDM) template. See Chapter 6, “Configuring SDM Templates.” This number represents the total of available MAC addresses, including those used for other Layer 2 functions and any other secure MAC addresses configured on interfaces.

Security Violations

It is a security violation when one of these situations occurs:

- The maximum number of secure MAC addresses have been added to the address table, and a station whose MAC address is not in the address table attempts to access the interface.
- An address learned or configured on one secure interface is seen on another secure interface in the same VLAN.

You can configure the interface for one of three violation modes, based on the action to be taken if a violation occurs:

- **protect**—when the number of secure MAC addresses reaches the maximum limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses to drop below the maximum value or increase the number of maximum allowable addresses. You are not notified that a security violation has occurred.

  
  Note: We do not recommend configuring the protect violation mode on a trunk port. The protect mode disables learning when any VLAN reaches its maximum limit, even if the port has not reached its maximum limit.

- **restrict**—when the number of secure MAC addresses reaches the maximum limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses to drop below the maximum value or increase the number of maximum allowable addresses. In this mode, you are notified that a security violation has occurred. An SNMP trap is sent, a syslog message is logged, and the violation counter increments.

- **shutdown**—a port security violation causes the interface to become error-disabled and to shut down immediately, and the port LED turns off. An SNMP trap is sent, a syslog message is logged, and the violation counter increments. When a secure port is in the error-disabled state, you can bring it out of this state by entering the `errdisable recovery cause psecure-violation` global configuration command, or you can manually re-enable it by entering the `shutdown` and `no shutdown` interface configuration commands. This is the default mode.

Table 24-1 shows the violation mode and the actions taken when you configure an interface for port security.

<table>
<thead>
<tr>
<th>Violation Mode</th>
<th>Traffic is forwarded¹</th>
<th>Sends SNMP trap</th>
<th>Sends syslog message</th>
<th>Displays error message²</th>
<th>Violation counter increments</th>
<th>Shuts down port</th>
</tr>
</thead>
<tbody>
<tr>
<td>protect</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>restrict</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>shutdown</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

1. Packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses.
2. The switch returns an error message if you manually configure an address that would cause a security violation.
Default Port Security Configuration

Table 24-2 shows the default port security configuration for an interface.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port security</td>
<td>Disabled on a port.</td>
</tr>
<tr>
<td>Sticky address learning</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Maximum secure MAC addresses per port</td>
<td>1.</td>
</tr>
<tr>
<td>Violation mode</td>
<td>Shutdown. The port shuts down when the maximum</td>
</tr>
<tr>
<td></td>
<td>number of secure MAC addresses is exceeded.</td>
</tr>
<tr>
<td>Port security aging</td>
<td>Disabled. Aging time is 0.</td>
</tr>
<tr>
<td></td>
<td>Static aging is disabled.</td>
</tr>
<tr>
<td></td>
<td>Type is absolute.</td>
</tr>
</tbody>
</table>

Configuration Guidelines

Follow these guidelines when configuring port security:

- Port security can only be configured on static access ports, trunk ports, or tunnel ports. A secure port cannot be a dynamic access port.
- A secure port cannot be a destination port for Switched Port Analyzer (SPAN).
- A secure port cannot belong to a Fast EtherChannel or a Gigabit EtherChannel port group.
- You cannot configure static secure or sticky secure MAC addresses in the voice VLAN.
- Voice VLAN is only supported on access ports and not on trunk ports, even though the configuration is allowed.

- A secure port cannot be a private-VLAN port.
- When you enable port security on an interface that is also configured with a voice VLAN, set the maximum allowed secure addresses on the port to two. When the port is connected to a Cisco IP phone, the IP phone requires one MAC address. The Cisco IP phone address is learned on the voice VLAN, but is not learned on the access VLAN. If you connect a single PC to the Cisco IP phone, no additional MAC addresses are required. If you connect more than one PC to the Cisco IP phone, you must configure enough secure addresses to allow one for each PC and one for the phone.
- If any type of port security is enabled on the access VLAN, dynamic port security is automatically enabled on the voice VLAN. You cannot configure port security on a per-VLAN basis.
- When a trunk port configured with port security and assigned to an access VLAN for data traffic and to a voice VLAN for voice traffic, entering the `switchport voice` and `switchport priority extend` interface configuration commands has no effect.

When a connected device uses the same MAC address to request an IP address for the access VLAN and then an IP address for the voice VLAN, only the access VLAN is assigned an IP address.
- When a voice VLAN is configured on a secure port that is also configured as a sticky secure port, all addresses on the voice VLAN are learned as dynamic secure addresses, and all addresses seen on the access VLAN to which the port belongs are learned as sticky secure addresses.

- When you enter a maximum secure address value for an interface, and the new value is greater than the previous value, the new value overwrites the previously configured value. If the new value is less than the previous value and the number of configured secure addresses on the interface exceeds the new value, the command is rejected.

- The switch does not support port security aging of sticky secure MAC addresses.

### Enabling and Configuring Port Security

Beginning in privileged EXEC mode, follow these steps to restrict input to an interface by limiting and identifying MAC addresses of the stations allowed to access the port:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>switchport mode {access</td>
</tr>
<tr>
<td>Step 4</td>
<td>switchport port-security</td>
</tr>
<tr>
<td>Step 5</td>
<td>switchport port-security maximum value [vlan [vlan-list]]</td>
</tr>
</tbody>
</table>

- `vlan`—set a per-VLAN maximum value.
- `vlan vlan-list`—set a per-VLAN maximum value on a range of VLANs separated by a hyphen, or a series of VLANs separated by commas. For non-specified VLANs, the per-VLAN maximum value is used.
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 6    | switchport port-security violation <br/>  { protect | restrict | shutdown } | (Optional) Set the violation mode, the action to be taken when a security violation is detected, as one of these:  
  - **protect**—When the number of port secure MAC addresses reaches the maximum limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses to drop below the maximum value or increase the number of maximum allowable addresses. You are not notified that a security violation has occurred.  
  - **restrict**—When the number of secure MAC addresses reaches the limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses or increase the number of maximum allowable addresses. An SNMP trap is sent, a syslog message is logged, and the violation counter increments.  
  - **shutdown**—The interface is error-disabled when a violation occurs, and the port LED turns off. An SNMP trap is sent, a syslog message is logged, and the violation counter increments.  
  **Note** We do not recommend configuring the protect mode on a trunk port. The protect mode disables learning when any VLAN reaches its maximum limit, even if the port has not reached its maximum limit.  
  **Note** When a secure port is in the error-disabled state, you can bring it out of this state by entering the `errdisable recovery cause psecure-violation` global configuration command, or you can manually re-enable it by entering the `shutdown` and `no shutdown` interface configuration commands. |
| 7    | switchport port-security <br/>  mac-address mac-address <br/>  [vlan vlan-id] | (Optional) Enter a secure MAC address for the interface. You can use this command to enter the maximum number of secure MAC addresses. If you configure fewer secure MAC addresses than the maximum, the remaining MAC addresses are dynamically learned.  
  (Optional) On a trunk port, you can specify the VLAN ID and the MAC address. If no VLAN ID is specified, the native VLAN is used.  
  **Note** If you enable sticky learning after you enter this command, the secure addresses that were dynamically learned are converted to sticky secure MAC addresses and are added to the running configuration. |
| 8    | switchport port-security <br/>  mac-address sticky | (Optional) Enable sticky learning on the interface. |
| 9    | switchport port-security <br/>  mac-address sticky mac-address | (Optional) Enter a sticky secure MAC address, repeating the command as many times as necessary. If you configure fewer secure MAC addresses than the maximum, the remaining MAC addresses are dynamically learned, are converted to sticky secure MAC addresses, and are added to the running configuration.  
  **Note** If you do not enable sticky learning before this command is entered, an error message appears, and you cannot enter a sticky secure MAC address. |
| 10   | end | Return to privileged EXEC mode. |
To return the interface to the default condition as not a secure port, use the `no switchport port-security` interface configuration command. If you enter this command when sticky learning is enabled, the sticky secure addresses remain part of the running configuration but are removed from the address table. All addresses are now dynamically learned.

To return the interface to the default number of secure MAC addresses, use the `no switchport port-security maximum value` interface configuration command. To return the violation mode to the default condition (shutdown mode), use the `no switchport port-security violation {protocol | restrict}` interface configuration command.

To disable sticky learning on an interface, use the `no switchport port-security mac-address sticky` interface configuration command. The interface converts the sticky secure MAC addresses to dynamic secure addresses. However, if you have previously saved the configuration with the sticky MAC addresses, you should save the configuration again after entering the `no switchport port-security` command, or the sticky addresses will be restored if the switch reboots.

To delete a specific secure MAC address from the address table, use the `no switchport port-security mac-address mac-address` interface configuration command. To delete all dynamic secure addresses on an interface from the address table, enter the `no switchport port-security` command followed by the `switchport port-security` command (to re-enable port security on the interface). If you use the `no switchport port-security mac-address sticky` interface configuration command to convert sticky secure MAC addresses to dynamic secure MAC addresses before entering the `no switchport port-security` command, all secure addresses on the interface except those that were manually configured are deleted.

You must specifically delete configured secure MAC addresses from the address table by using the `no switchport port-security mac-address mac-address` interface configuration command.

This example shows how to enable port security on an interface and to set the maximum number of secure addresses to 50. The violation mode is the default, no static secure MAC addresses are configured, and sticky learning is enabled.

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 50
Switch(config-if)# switchport port-security mac-address sticky
```

This example shows how to configure a static secure MAC address on VLAN 3 on an interface:

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address 0000.02000.0004 vlan 3
```

### Command Purpose

<table>
<thead>
<tr>
<th>Step 11</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show port-security</td>
<td>Verify your entries.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 12</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
Enabling and Configuring Port Security Aging

You can use port security aging to set the aging time for all secure addresses on a port. Two types of aging are supported per port:

- **Absolute**—The secure addresses on the port are deleted after the specified aging time.
- **Inactivity**—The secure addresses on the port are deleted only if the secure addresses are inactive for the specified aging time.

Use this feature to remove and add devices on a secure port without manually deleting the existing secure MAC addresses and to still limit the number of secure addresses on a port. You can enable or disable the aging of secure addresses on a per-port basis.

Beginning in privileged EXEC mode, follow these steps to configure port security aging:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>switchport port-security aging {static</td>
</tr>
</tbody>
</table>

**Note** The switch does not support port security aging of sticky secure addresses.

Enter **static** to enable aging for statically configured secure addresses on this port.

For **time**, specify the aging time for this port. The valid range is from 1 to 1440 minutes.

For **type**, select one of these keywords:

- **absolute**—Sets the aging type as absolute aging. All the secure addresses on this port age out exactly after the time (minutes) specified lapses and are removed from the secure address list.
- **inactivity**—Sets the aging type as inactivity aging. The secure addresses on this port age out only if there is no data traffic from the secure source addresses for the specified time period.

| **Step 4** | end | Return to privileged EXEC mode. |
| **Step 5** | show port-security [interface interface-id] [address] | Verify your entries. |
| **Step 6** | copy running-config startup-config | (Optional) Save your entries in the configuration file. |

To disable port security aging for all secure addresses on a port, use the **no switchport port-security aging time** interface configuration command. To disable aging for only statically configured secure addresses, use the **no switchport port-security aging static** interface configuration command.

This example shows how to set the aging time as 2 hours for the secure addresses on an interface:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# switchport port-security aging time 120
```
This example shows how to set the aging time as 2 minutes for the inactivity aging type with aging enabled for the configured secure addresses on the interface:

```
Switch(config-if)# switchport port-security aging time 2
Switch(config-if)# switchport port-security aging type inactivity
Switch(config-if)# switchport port-security aging static
```

You can verify the previous commands by entering the `show port-security interface interface-id` privileged EXEC command.

## Port Security and Private VLANs

Port security allows an administrator to limit the number of MAC addresses learned on a port or to define which MAC addresses can be learned on a port.

Beginning in privileged EXEC mode, follow these steps to configure port security on a PVLAN host and promiscuous ports:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface <em>interface-id</em></td>
<td>Specify the interface to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>switchport mode private-vlan (host</td>
<td>promiscuous)</td>
</tr>
<tr>
<td>Step 4</td>
<td>switchport port-security</td>
<td>Enable port security on the interface.</td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 6</td>
<td>show port-security [interface <em>interface-id</em>] [address]</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 7</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

```
Switch(config)# interface GigabitEthernet 1/0/8
Switch(config-if)# switchport private-vlan mapping 2061 2201-2206,3101
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport port-security maximum 288
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security violation restrict
```

**Note**

Ports that have both port security and private VLANs configured can be labeled secure PVLAN ports. When a secure address is learned on a secure PVLAN port, the same secure address cannot be learned on another secure PVLAN port belonging to the same primary VLAN. However, an address learned on insecure PVLAN port can be learned on a secure PVLAN port belonging to same primary VLAN.

Secure addresses that are learned on host port get automatically replicated on associated primary VLANs, and similarly, secure addresses learned on promiscuous ports automatically get replicated on all associated secondary VLANs. Static addresses (using `mac-address-table static` command) cannot be user configured on a secure port. Displaying Port-Based Traffic Control Settings
The `show interfaces interface-id switchport` privileged EXEC command displays (among other characteristics) the interface traffic suppression and control configuration. The `show storm-control` and `show port-security` privileged EXEC commands display those features.

To display traffic control information, use one or more of the privileged EXEC commands in Table 24-3.

**Table 24-3 Commands for Displaying Traffic Control Status and Configuration**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show interfaces [interface-id] switchport</code></td>
<td>Displays the administrative and operational status of all switching (nonrouting) ports or the specified port, including port blocking and port protection settings.</td>
</tr>
<tr>
<td>`show storm-control [interface-id] [broadcast</td>
<td>multicast</td>
</tr>
<tr>
<td><code>show port-security [interface interface-id]</code></td>
<td>Displays port security settings for the switch or for the specified interface, including the maximum allowed number of secure MAC addresses for each interface, the number of secure MAC addresses on the interface, the number of security violations that have occurred, and the violation mode.</td>
</tr>
<tr>
<td><code>show port-security [interface interface-id] address</code></td>
<td>Displays all secure MAC addresses configured on all switch interfaces or on a specified interface with aging information for each address.</td>
</tr>
<tr>
<td><code>show port-security interface interface-id vlan</code></td>
<td>Displays the number of secure MAC addresses configured per VLAN on the specified interface.</td>
</tr>
</tbody>
</table>
25

Configuring CDP

This chapter describes how to configure Cisco Discovery Protocol (CDP) on the Catalyst 3750 Metro switch.

For complete syntax and usage information for the commands used in this chapter, see the command reference for this release and the “System Management Commands” section in the Cisco IOS Configuration Fundamentals Command Reference, Release 12.2.

This chapter consists of these sections:
- Understanding CDP, page 25-1
- Configuring CDP, page 25-2
- Monitoring and Maintaining CDP, page 25-4

Understanding CDP

CDP is a device discovery protocol that runs over Layer 2 (the data link layer) on all Cisco-manufactured devices (routers, bridges, access servers, and switches) and allows network management applications to discover Cisco devices that are neighbors of already known devices. With CDP, network management applications can learn the device type and the Simple Network Management Protocol (SNMP) agent address of neighboring devices running lower-layer, transparent protocols. This feature enables applications to send SNMP queries to neighboring devices.

CDP runs on all media that support Subnetwork Access Protocol (SNAP). Because CDP runs over the data-link layer only, two systems that support different network-layer protocols can learn about each other.

Each CDP-configured device sends periodic messages to a multicast address, advertising at least one address at which it can receive SNMP messages. The advertisements also contain time-to-live, or holdtime information, which is the length of time a receiving device holds CDP information before discarding it. Each device also listens to the messages sent by other devices to learn about neighboring devices.

For a switch and connected endpoint devices running Cisco Medianet
- CDP identifies connected endpoints that communicate directly with the switch.
- To prevent duplicate reports of neighboring devices, only one wired switch reports the location information.

## Configuring CDP

These sections include CDP configuration information and procedures:

- Default CDP Configuration, page 25-2
- Configuring the CDP Characteristics, page 25-2
- Disabling and Enabling CDP, page 25-3
- Disabling and Enabling CDP on an Interface, page 25-4

### Default CDP Configuration

Table 25-1 shows the default CDP configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDP global state</td>
<td>Enabled</td>
</tr>
<tr>
<td>CDP interface state</td>
<td>Enabled</td>
</tr>
<tr>
<td>CDP timer (packet update frequency)</td>
<td>60 seconds</td>
</tr>
<tr>
<td>CDP holdtime (before discarding)</td>
<td>180 seconds</td>
</tr>
<tr>
<td>CDP Version-2 advertisements</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

### Configuring the CDP Characteristics

You can configure the frequency of CDP updates, the amount of time to hold the information before discarding it, and whether or not to send Version-2 advertisements.

Beginning in privileged EXEC mode, follow these steps to configure the CDP timer, holdtime, and advertisement type.

**Note**

Steps 2 through 4 are all optional and can be performed in any order.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 cdp timer seconds</td>
<td>(Optional) Set the transmission frequency of CDP updates in seconds. The range is 5 to 254; the default is 60 seconds.</td>
</tr>
</tbody>
</table>
Use the `no` form of the CDP commands to return to the default settings.

This example shows how to configure and verify CDP characteristics.

```
Switch# configure terminal
Switch(config)# cdp timer 50
Switch(config)# cdp holdtime 120
Switch(config)# cdp advertise-v2
Switch(config)# end

Switch# show cdp
Global CDP information:
  Sending CDP packets every 50 seconds
  Sending a holdtime value of 120 seconds
  Sending CDPv2 advertisements is enabled
```

For additional CDP `show` commands, see the “Monitoring and Maintaining CDP” section on page 25-4.

## Disabling and Enabling CDP

CDP is enabled by default.

Beginning in privileged EXEC mode, follow these steps to disable the CDP device discovery capability:

### Command Purpose

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><code>no cdp run</code></td>
<td>Disable CDP.</td>
</tr>
<tr>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

Beginning in privileged EXEC mode, follow these steps to enable CDP when it has been disabled:

### Command Purpose

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><code>cdp run</code></td>
<td>Enable CDP after disabling it.</td>
</tr>
<tr>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
This example shows how to enable CDP if it has been disabled.

Switch# configure terminal
Switch(config)# cdp run
Switch(config)# end

Disabling and Enabling CDP on an Interface

CDP is enabled by default on all supported interfaces to send and receive CDP information.
Beginning in privileged EXEC mode, follow these steps to disable CDP on an interface:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Enter interface configuration mode, and enter the interface on which you are disabling CDP.</td>
</tr>
<tr>
<td>Step 3 no cdp enable</td>
<td>Disable CDP on an interface.</td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Beginning in privileged EXEC mode, follow these steps to enable CDP on an interface when it has been disabled:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Enter interface configuration mode, and enter the interface on which you are enabling CDP.</td>
</tr>
<tr>
<td>Step 3 cdp enable</td>
<td>Enable CDP on an interface after disabling it.</td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

This example shows how to enable CDP on a port when it has been disabled.

Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# cdp enable
Switch(config-if)# end

Monitoring and Maintaining CDP

To monitor and maintain CDP on your device, perform one or more of these tasks, beginning in privileged EXEC mode.
This is an example of the output from the `show cdp` privileged EXEC commands:

```
Switch# show cdp
Global CDP information:
   Sending CDP packets every 50 seconds
   Sending a holdtime value of 120 seconds
   Sending CDPv2 advertisements is enabled
```
This chapter describes how to configure the Link Layer Discovery Protocol (LLDP) and LLDP Media Endpoint Discovery (LLDP-MED) on the Catalyst 3750 Metro switch. Unless otherwise noted, the term switch refers to a standalone switch and to a switch stack.

For complete syntax and usage information for the commands used in this chapter, see the command reference for this release and the “System Management Commands” section in the Cisco IOS Configuration Fundamentals Command Reference, Release 12.2.

This chapter consists of these sections:
- Understanding LLDP and LLDP-MED, page 26-1
- Configuring LLDP and LLDP-MED, page 26-3
- Monitoring and Maintaining LLDP and LLDP-MED, page 26-7

Understanding LLDP and LLDP-MED

This section contains this conceptual information:
- Understanding LLDP, page 26-1
- Understanding LLDP-MED, page 26-2

Understanding LLDP

The Cisco Discovery Protocol (CDP) is a device discovery protocol that runs over Layer 2 (the data link layer) on all Cisco-manufactured devices (routers, bridges, access servers, and switches). CDP allows network management applications to automatically discover and learn about other Cisco devices connected to the network.

To support non-Cisco devices and to allow for interoperability between other devices, the switch supports the IEEE 802.1AB Link Layer Discovery Protocol (LLDP). LLDP is a neighbor discovery protocol that is used for network devices to advertise information about themselves to other devices on the network. This protocol runs over the data-link layer, which allows two systems running different network layer protocols to learn about each other.
LLDP supports a set of attributes that it uses to discover neighbor devices. These attributes contain type, length, and value descriptions and are referred to as TLVs. LLDP supported devices can use TLVs to receive and send information to their neighbors. Details such as configuration information, device capabilities, and device identity can be advertised using this protocol.

The switch supports these basic management TLVs. These are mandatory LLDP TLVs.

- Port description TLV
- System name TLV
- System description
- System capabilities TLV
- Management address TLV

These organizationally specific LLDP TLVs are also advertised to support LLDP-MED.

- Port VLAN ID TLV (IEEE 802.1 organizationally specific TLVs)
- MAC/PHY configuration/status TLV (IEEE 802.3 organizationally specific TLVs)

Note

A switch stack appears as a single switch in the network. Therefore, LLDP discovers the switch stack, not the individual stack members.

Understanding LLDP-MED

LLDP for Media Endpoint Devices (LLDP-MED) is an extension to LLDP that operates between endpoint devices such as IP phones and network devices such as switches. It specifically provides support for voice over IP (VoIP) applications and provides additional TLVs for capabilities discovery, network policy, Power over Ethernet, and inventory management.

LLDP-MED supports these TLVs:

- LLDP-MED capabilities TLV
  Allows LLDP-MED endpoints to determine the capabilities that the connected device supports and what capabilities the device has enabled.

- Network policy TLV
  Allows both network connectivity devices and endpoints to advertise VLAN configurations and associated Layer 2 and Layer 3 attributes for the specific application on that port. For example, the switch can notify a phone of the VLAN number that it should use. The phone can connect into any switch, obtain its VLAN number, and then start communicating with the call control.

- Power management TLV
  Enables advanced power management between LLDP-MED endpoint and network connectivity devices. Allows switches and phones to convey power information, such as how the device is powered, power priority, and how much power the device needs.

- Inventory management TLV
  Allows an endpoint to transmit detailed inventory information about itself to the switch, including information hardware revision, firmware version, software version, serial number, manufacturer name, model name, and asset ID TLV.
- Location TLV
  Provides location information from the switch to the endpoint device. The location TLV can send this information:
  - Civic location information
    Provides the civic address information and postal information. Examples of civic location information are street address, road name, and postal community name information.
  - ELIN location information
    Provides the location information of a caller. The location is determined by the Emergency location identifier number (ELIN), which is a phone number that routes an emergency call to the local public safety answering point (PSAP) and which the PSAP can use to call back the emergency caller.

### Configuring LLDP and LLDP-MED

This section contains this configuration information:

- Default LLDP Configuration, page 26-3
- Configuring LLDP Characteristics, page 26-4
- Disabling and Enabling LLDP Globally, page 26-5
- Disabling and Enabling LLDP on an Interface, page 26-5
- Configuring LLDP-MED TLVs, page 26-6

### Default LLDP Configuration

Table 26-1 shows the default LLDP configuration. To change the default settings, use the LLDP global configuration and LLDP interface configuration commands.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>LLDP global state</td>
<td>Disabled</td>
</tr>
<tr>
<td>LLDP holdtime (before discarding)</td>
<td>120 seconds</td>
</tr>
<tr>
<td>LLDP timer (packet update frequency)</td>
<td>30 seconds</td>
</tr>
<tr>
<td>LLDP reinitialization delay</td>
<td>2 seconds</td>
</tr>
<tr>
<td>LLDP tlv-select</td>
<td>Disabled to send and receive all TLVs.</td>
</tr>
<tr>
<td>LLDP interface state</td>
<td>Disabled</td>
</tr>
<tr>
<td>LLDP receive</td>
<td>Disabled</td>
</tr>
<tr>
<td>LLDP transmit</td>
<td>Disabled</td>
</tr>
<tr>
<td>LLDP med-tlv-select</td>
<td>Disabled to send all LLDP-MED TLVs</td>
</tr>
</tbody>
</table>
Configuring LLDP Characteristics

You can configure the frequency of LLDP updates, the amount of time to hold the information before discarding it, and the initialization delay time. You can also select the LLDP and LLDP-MED TLVs to be sent and received.

Beginning in privileged EXEC mode, follow these steps to configure these characteristics:

### Note
Steps 2 through 5 are all optional and can be performed in any order.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>lldp holdtime seconds</strong></td>
</tr>
<tr>
<td></td>
<td>(Optional) Specify the amount of time a receiving device should hold the information sent by your device before discarding it. The range is 0 to 65535 seconds; the default is 120 seconds.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>lldp reinit</strong></td>
</tr>
<tr>
<td></td>
<td>(Optional) Specify the delay time in seconds for LLDP to initialize on any interface. The range is 2 to 5 seconds; the default is 2 seconds.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>lldp timer seconds</strong></td>
</tr>
<tr>
<td></td>
<td>(Optional) Set the transmission frequency of LLDP updates in seconds. The range is 5 to 65534 seconds; the default is 30 seconds.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>lldp tlv-select</strong></td>
</tr>
<tr>
<td></td>
<td>(Optional) Specify the LLDP TLVs to send or receive.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>interface interface-id</strong></td>
</tr>
<tr>
<td></td>
<td>Specify the interface on which you are enabling LLDP, and enter interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>lldp med-tlv-select</strong></td>
</tr>
<tr>
<td></td>
<td>(Optional) Specify the LLDP-MED TLVs to send or receive.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><strong>copy running-config startup-config</strong></td>
</tr>
<tr>
<td></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Use the **no** form of each of the LLDP commands to return to the default setting.

This example shows how to configure LLDP characteristics.

```
Switch# configure terminal
Switch(config)# lldp holdtime 120
Switch(config)# lldp reinit 2
Switch(config)# lldp timer 30
Switch(config)# end
```

For additional LLDP **show** commands, see the “Monitoring and Maintaining LLDP and LLDP-MED” section on page 26-7.
Disabling and Enabling LLDP Globally

LLDP is disabled by default.

Beginning in privileged EXEC mode, follow these steps to globally disable LLDP:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td>Step 2</td>
<td><strong>no lldp run</strong></td>
</tr>
<tr>
<td>Step 3</td>
<td><strong>end</strong></td>
</tr>
</tbody>
</table>

Beginning in privileged EXEC mode, follow these steps to enable LLDP-MED when it has been disabled:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td>Step 2</td>
<td><strong>lldp run</strong></td>
</tr>
<tr>
<td>Step 3</td>
<td><strong>end</strong></td>
</tr>
</tbody>
</table>

This example shows how to globally disable LLDP.

```
Switch# configure terminal
Switch(config)# no lldp run
Switch(config)# end
```

This example shows how to globally enable LLDP.

```
Switch# configure terminal
Switch(config)# lldp run
Switch(config)# end
```

Disabling and Enabling LLDP on an Interface

LLDP is disabled by default on all supported interfaces to send and to receive LLDP information.

**Note**

If the interface is configured as a tunnel port, LLDP is automatically disabled.

Beginning in privileged EXEC mode, follow these steps to disable LLDP on an interface.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td>Step 2</td>
<td><strong>interface interface-id</strong></td>
</tr>
<tr>
<td>Step 3</td>
<td><strong>no lldp transmit</strong></td>
</tr>
<tr>
<td>Step 4</td>
<td><strong>no lldp receive</strong></td>
</tr>
</tbody>
</table>
Beginning in privileged EXEC mode, follow these steps to enable LLDP on an interface when it has been disabled:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><code>interface interface-id</code></td>
<td>Specify the interface on which you are enabling LLDP-MED, and enter interface configuration mode.</td>
</tr>
<tr>
<td><code>lldp transmit</code></td>
<td>LLDP packets are sent on the interface.</td>
</tr>
<tr>
<td><code>lldp receive</code></td>
<td>LLDP packets are received on the interface.</td>
</tr>
<tr>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

This example shows how to enable LLDP on an interface.
```
Switch# configure terminal
Switch(config)# interface GigabitEthernet1/0/1
Switch(config-if)# lldp transmit
Switch(config-if)# lldp receive
Switch(config-if)# end
```

### Configuring LLDP-MED TLVs

By default, the switch only sends LLDP packets until it receives LLDP-MED packets from the end device. It will then send LLDP packets with MED TLVs as well. When the LLDP-MED entry has been aged out, it only sends LLDP packets again.

By using the `lldp` interface command, you can configure the interface not to send the TLVs listed in Table 26-2.

<table>
<thead>
<tr>
<th>LLDP-MED TLV</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>inventory-management</td>
<td>LLDP-MED inventory management TLV</td>
</tr>
<tr>
<td>location</td>
<td>LLDP-MED location TLV</td>
</tr>
<tr>
<td>network-policy</td>
<td>LLDP-MED network policy TLV</td>
</tr>
<tr>
<td>power-management</td>
<td>LLDP-MED power management TLV</td>
</tr>
</tbody>
</table>
Beginning in privileged EXEC mode, follow these steps to disable a TLV on an interface:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Specify the interface on which you are configuring a LLDP-MED TLV, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3 no lldp med-tlv-select tlv</td>
<td>Specify the TLV to disable.</td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Beginning in privileged EXEC mode, follow these steps to enable a TLV on an interface:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Specify the interface on which you are configuring an LLDP-MED TLV, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3 lldp med-tlv-select tlv</td>
<td>Specify the TLV to enable.</td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

This example shows how to enable a TLV on an interface when it has been disabled.

Switch# configure terminal
Switch(config)# interface GigabitEthernet1/0/1
Switch(config-if)# lldp med-tlv-select inventory-management
Switch(config-if)# end

Monitoring and Maintaining LLDP and LLDP-MED

To monitor and maintain LLDP and LLDP-MED on your device, perform one or more of these tasks, beginning in privileged EXEC mode.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear lldp counters</td>
<td>Reset the traffic counters to zero.</td>
</tr>
<tr>
<td>clear lldp table</td>
<td>Delete the LLDP table of information about neighbors.</td>
</tr>
<tr>
<td>show lldp</td>
<td>Display global information, such as frequency of transmissions, the holdtime for packets being sent, and the delay time for LLDP to initialize on an interface.</td>
</tr>
</tbody>
</table>
| show lldp entry entry-name | Display information about a specific neighbor.  
You can enter an asterisk (*) to display all neighbors, or you can enter the name of the neighbor about which you want information. |
| show lldp interface [interface-id] | Display information about interfaces where LLDP is enabled.  
You can limit the display to the interface about which you want information. |
Monitoring and Maintaining LLDP and LLDP-MED

Chapter 26  Configuring LLDP and LLDP-MED

display information about neighbors, including device type, interface type and number, holdtime settings, capabilities, and port ID. You can limit the display to neighbors of a specific interface or expand the display to provide more detailed information.

**show lldp traffic**

Display LLDP counters, including the number of packets sent and received, number of packets discarded, and number of unrecognized TLVs.
Configuring UDLD

This chapter describes how to configure the UniDirectional Link Detection (UDLD) protocol on the Catalyst 3750 Metro switch.

Note

For complete syntax and usage information for the commands used in this chapter, see the command reference for this release.

This chapter consists of these sections:
- Understanding UDLD, page 27-1
- Configuring UDLD, page 27-4
- Displaying UDLD Status, page 27-6

Understanding UDLD

UDLD is a Layer 2 protocol that enables devices connected through fiber-optic or twisted-pair Ethernet cables to monitor the physical configuration of the cables and detect when a unidirectional link exists. All connected devices must support UDLD for the protocol to successfully identify and disable unidirectional links. When UDLD detects a unidirectional link, it administratively shuts down the affected interface and alerts you. Unidirectional links can cause a variety of problems, including spanning-tree topology loops.

Modes of Operation

UDLD supports two modes of operation: normal (the default) and aggressive. In normal mode, UDLD can detect unidirectional links due to misconnected ports on fiber-optic connections. In aggressive mode, UDLD also can detect unidirectional links due to one-way traffic on fiber-optic and on twisted-pair links and to misconnected ports on fiber-optic links.

In normal and in aggressive mode, UDLD works with the Layer 1 mechanisms to learn the physical status of a link. At Layer 1, autonegotiation takes care of physical signaling and fault detection. UDLD performs tasks that autonegotiation cannot perform, such as detecting the identities of neighbors and shutting down misconnected interfaces. When you enable both autonegotiation and UDLD, the Layer 1 and Layer 2 detections work together to prevent physical and logical unidirectional connections and the malfunctioning of other protocols.
A unidirectional link occurs whenever traffic sent by a local device is received by its neighbor but traffic from the neighbor is not received by the local device.

In normal mode, UDLD can detect a unidirectional link when fiber strands in a fiber-optic port are misconnected and the Layer 1 mechanisms do not detect this misconnection. If the ports are connected correctly but the traffic is one way, UDLD does not detect the unidirectional link because the Layer 1 mechanism, which is supposed to detect this condition, does not do so. In this case, the logical link is considered undetermined, and UDLD does not disable the interface.

When UDLD is in normal mode, if one of the fiber strands in a pair is disconnected, as long as autonegotiation is active, the link does not stay up because the Layer 1 mechanisms detect a physical problem with the link. In this case, UDLD does not take any action and the logical link is considered undetermined.

In aggressive mode, UDLD can detect a unidirectional link by using the previous detection methods. UDLD in aggressive mode also can detect a unidirectional link on a point-to-point link on which no failure between the two devices is allowed. It also can detect a unidirectional link when one of these problems exists:

- On fiber-optic or twisted-pair links, one of the interfaces cannot send or receive traffic.
- On fiber-optic or twisted-pair links, one of the interfaces is down while the other is up.
- One of the fiber strands in a pair is disconnected.

In these cases, UDLD shuts down the affected interface.

In a point-to-point link, UDLD hello packets can be considered as a heart beat whose presence guarantees the health of the link. Conversely, the loss of the heart beat means that the link must be shut down if it is not possible to re-establish a bidirectional link.

If both fibers are working normally from a Layer 1 perspective, UDLD in aggressive mode detects whether those fibers are connected correctly and whether traffic is flowing bidirectionally between the correct neighbors. This check cannot be performed by autonegotiation because autonegotiation operates at Layer 1.

### Methods to Detect Unidirectional Links

UDLD operates by using two mechanisms:

- Neighbor database maintenance
  
  UDLD learns about other UDLD-capable neighbors by periodically sending a hello packet (also called an advertisement or probe) on every active interface to keep each device informed about its neighbors.

  When the switch receives a hello message, it caches the information until the age time (hold time or time-to-live) expires. If the switch receives a new hello message before an older cache entry ages, the switch replaces the older entry with the new one.

  Whenever an interface is disabled and UDLD is running, whenever UDLD is disabled on an interface, or whenever the switch is reset, UDLD clears all existing cache entries for the interfaces affected by the configuration change. UDLD sends at least one message to inform the neighbors to flush the part of their caches affected by the status change. The message is intended to keep the caches synchronized.
• Event-driven detection and echoing

UDLD relies on echoing as its detection mechanism. Whenever a UDLD device learns about a new neighbor or receives a resynchronization request from an out-of-sync neighbor, it restarts the detection window on its side of the connection and sends echo messages in reply. Because this behavior is the same on all UDLD neighbors, the sender of the echoes expects to receive an echo in reply.

If the detection window ends and no valid reply message is received, the link might shut down, depending on the UDLD mode. When UDLD is in normal mode, the link might be considered undetermined and might not shut down. When UDLD is in aggressive mode, the link is considered unidirectional, and the interface is shut down.

If UDLD in normal mode is in the advertisement or in the detection phase and all the neighbor cache entries are aged out, UDLD restarts the link-up sequence to resynchronize with any potentially out-of-sync neighbors.

If you enable aggressive mode when all the neighbors of an interface have aged out either in the advertisement or in the detection phase, UDLD restarts the link-up sequence to resynchronize with any potentially out-of-sync neighbor. UDLD shuts down the interface if, after the fast train of messages, the link state is still undetermined.

Figure 27-1 shows an example of a unidirectional link condition.

**Figure 27-1  UDLD Detection of a Unidirectional Link**

Switch B successfully receives traffic from Switch A on this port. However, Switch A does not receive traffic from Switch B on the same port. If UDLD is in aggressive mode, it detects the problem and disables the port. If UDLD is in normal mode, the logical link is considered undetermined, and UDLD does not disable the interface.
Configuring UDLD

This section describes how to configure UDLD on your switch. It contains this configuration information:

- Default UDLD Configuration, page 27-4
- UDLD Configuration Guidelines, page 27-4
- Enabling UDLD Globally, page 27-5
- Enabling UDLD on an Interface, page 27-5
- Resetting an Interface Disabled by UDLD, page 27-6

Default UDLD Configuration

Table 27-1 shows the default UDLD configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDLD global enable state</td>
<td>Globally disabled</td>
</tr>
<tr>
<td>UDLD per-port enable state for fiber-optic media</td>
<td>Disabled on all Ethernet fiber-optic ports</td>
</tr>
<tr>
<td>UDLD per-port enable state for twisted-pair (copper) media</td>
<td>Disabled on all Ethernet 10/100 and 1000BASE-TX ports</td>
</tr>
<tr>
<td>UDLD aggressive mode</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

UDLD Configuration Guidelines

These are the UDLD configuration guidelines:

- UDLD is not supported on ATM ports.
- A UDLD-capable interface also cannot detect a unidirectional link if it is connected to a UDLD-incapable interface of another switch.
- When configuring the mode (normal or aggressive), make sure that the same mode is configured on both sides of the link.

Caution

Loop guard works only on point-to-point links. We recommend that each end of the link has a directly connected device that is running STP.
### Enabling UDLD Globally

- Beginning in privileged EXEC mode, follow these steps to enable UDLD in the aggressive or normal mode and to set the configurable message timer on all fiber-optic ports on the switch:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>**udld {aggressive</td>
</tr>
<tr>
<td></td>
<td>Specify the UDLD mode of operation:</td>
</tr>
<tr>
<td></td>
<td>• <strong>aggressive</strong>—Enables UDLD in aggressive mode on all fiber-optic ports.</td>
</tr>
<tr>
<td></td>
<td>• <strong>enable</strong>—Enables UDLD in normal mode on all fiber-optic ports on the switch. UDLD is disabled by default.</td>
</tr>
<tr>
<td></td>
<td>An individual interface configuration overrides the setting of the <strong>udld enable</strong> global configuration command.</td>
</tr>
<tr>
<td></td>
<td>For more information about aggressive and normal modes, see the “Modes of Operation” section on page 27-1.</td>
</tr>
<tr>
<td></td>
<td>• <strong>message time</strong> message-timer-interval—Configures the period of time between UDLD probe messages on interfaces that are in the advertisement phase and are detected to be bidirectional. The range is 1 to 90 seconds.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>This command affects fiber-optic ports only. Use the <strong>udld</strong> interface configuration command to enable UDLD on other interface types. For more information, see the “Enabling UDLD on an Interface” section on page 27-5.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>end</strong></td>
</tr>
<tr>
<td></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>show udld</strong></td>
</tr>
<tr>
<td></td>
<td>Verify your entries.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>copy running-config startup-config</strong></td>
</tr>
<tr>
<td></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable UDLD globally, use the **no udld enable** global configuration command to disable normal mode UDLD on all fiber-optic ports. Use the **no udld aggressive** global configuration command to disable aggressive mode UDLD on all fiber-optic ports.

### Enabling UDLD on an Interface

Beginning in privileged EXEC mode, follow these steps either to enable UDLD in the aggressive or normal mode or to disable UDLD on an interface:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>interface interface-id</strong></td>
</tr>
<tr>
<td></td>
<td>Specify the interface to be enabled for UDLD, and enter interface configuration mode.</td>
</tr>
</tbody>
</table>
### Resetting an Interface Disabled by UDLD

Beginning in privileged EXEC mode, follow these steps to reset all interfaces disabled by UDLD:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>udld reset</td>
<td>Reset all interfaces disabled by UDLD.</td>
</tr>
<tr>
<td>2</td>
<td>show udld</td>
<td>Verify your entries.</td>
</tr>
</tbody>
</table>

You can also bring up the interface by using these commands:

- **The shutdown** interface configuration command followed by the **no shutdown** interface configuration command restarts the disabled interface.
- **The no udld** `aggressive | enable` global configuration command followed by the **udld** `aggressive | enable` global configuration command re-enables the disabled interfaces.
- **The udld port disable** interface configuration command followed by the **udld port** `aggressive` interface configuration command re-enables the disabled fiber-optic port.
- **The errdisable recovery cause udld** global configuration command enables the timer to automatically recover from the UDLD error-disabled state, and the **errdisable recovery interval** global configuration command specifies the time to recover from the UDLD error-disabled state.

### Displaying UDLD Status

To display the UDLD status for the specified interface or for all interfaces, use the **show udld** `[interface-id]` privileged EXEC command.

For detailed information about the fields in the display, see the command reference for this release.
CHAPTER 28

Configuring SPAN and RSPAN

This chapter describes how to configure Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) on the Catalyst 3750 Metro switch.

Note
For complete syntax and usage information for the commands used in this chapter, see the command reference for this release.

This chapter consists of these sections:
- Understanding SPAN and RSPAN, page 28-1
- Configuring SPAN and RSPAN, page 28-9
- Displaying SPAN and RSPAN Status, page 28-23

Understanding SPAN and RSPAN

You can analyze network traffic passing through ports or VLANs by using SPAN or RSPAN to send a copy of the traffic to another port on the switch or on another switch that has been connected to a network analyzer or other monitoring or security device. SPAN copies (or mirrors) traffic received or sent (or both) on source ports or source VLANs to a destination port for analysis. SPAN does not affect the switching of network traffic on the source ports or VLANs. You must dedicate the destination port for SPAN use. Except for traffic that is required for the SPAN or RSPAN session, destination ports do not receive or forward traffic.

Only traffic that enters or leaves source ports or traffic that enters or leaves source VLANs can be monitored by using SPAN; traffic routed to a source VLAN cannot be monitored. For example, if incoming traffic is being monitored, traffic that gets routed from another VLAN to the source VLAN cannot be monitored; however, traffic that is received on the source VLAN and routed to another VLAN can be monitored.

Enhanced-services (ES) ports cannot be SPAN or RSPAN source ports.

You can use the SPAN or RSPAN destination port to inject traffic from a network security device. For example, if you connect a Cisco Intrusion Detection System (IDS) sensor appliance to a destination port, the IDS device can send TCP reset packets to close down the TCP session of a suspected attacker.
This section includes these topics:

- **Local SPAN**, page 28-2
- **Remote SPAN**, page 28-2
- **SPAN and RSPAN Concepts and Terminology**, page 28-3
- **SPAN and RSPAN Interaction with Other Features**, page 28-8

### Local SPAN

Local SPAN supports a SPAN session entirely within one switch; all source ports or source VLANs and destination ports reside in the same switch. Local SPAN copies traffic from one or more source ports in any VLAN or from one or more VLANs to a destination port for analysis. For example, in Figure 28-1, all traffic on port 5 (the source port) is mirrored to port 10 (the destination port). A network analyzer on port 10 receives all network traffic from port 5 without being physically attached to port 5.

**Figure 28-1  Example of Local SPAN Configuration on a Switch**

![Network analyzer](image)

### Remote SPAN

RSPAN supports source ports, source VLANs, and destination ports on different switches, enabling remote monitoring of multiple switches across your network. Figure 28-2 shows RSPAN source ports configured on Switch A and Switch B with RSPAN destination ports configured on Switch C. The traffic for each RSPAN session is carried over a user-specified RSPAN VLAN that is dedicated for that RSPAN session in all participating switches. The RSPAN traffic from the source ports or VLANs is copied into the RSPAN VLAN and forwarded over trunk ports carrying the RSPAN VLAN to a destination session monitoring the RSPAN VLAN. Each RSPAN source switch must have either ports or VLANs as RSPAN sources. The destination is always a physical port.
SPAN and RSPAN Concepts and Terminology

This section describes concepts and terminology associated with SPAN and RSPAN configuration.

SPAN Sessions

SPAN sessions (local or remote) allow you to monitor traffic on one or more ports, or one or more VLANs, and send the monitored traffic to one or more destination ports.

A local SPAN session is an association of a destination port with source ports or source VLANs, all on a single network device. Local SPAN does not have separate source and destination sessions. Local SPAN sessions gather a set of ingress and egress packets specified by the user and form them into a stream of SPAN data, which is directed to the destination port.

RSPAN consists of at least one RSPAN source session, an RSPAN VLAN, and at least one RSPAN destination session. You separately configure RSPAN source sessions and RSPAN destination sessions on different network devices. To configure an RSPAN source session on a device, you associate a set of source ports or source VLANs with an RSPAN VLAN. The output of this session is the stream of SPAN packets that are sent to the RSPAN VLAN. To configure an RSPAN destination session on another device, you associate the destination port with the RSPAN VLAN. The destination session collects all RSPAN VLAN traffic and sends it out the RSPAN destination port.
An RSPAN source session is very similar to a local SPAN session, except for where the packet stream is directed. In an RSPAN source session, SPAN packets are relabeled with the RSPAN VLAN ID and directed over normal trunk ports to the destination switch.

An RSPAN destination session takes all packets received on the RSPAN VLAN, strips off the VLAN tagging, and presents them on the destination port. Its purpose is to present a copy of all RSPAN VLAN packets (except Layer 2 control packets) to the user for analysis.

There can be more than one source session and more than one destination session active in the same RSPAN VLAN. There can also be intermediate switches separating the RSPAN source and destination sessions. These switches need not be capable of running RSPAN, but they must handle the requirements of the RSPAN VLAN (see the “RSPAN VLAN” section on page 28-8).

Traffic monitoring in a SPAN session has these restrictions:

- Sources can be ports or VLANs, but you cannot mix source ports and source VLANs in the same session.
- The switch supports up to two source sessions (local SPAN and RSPAN source sessions). You can run both a local SPAN and an RSPAN source session in the same switch. The switch supports a total of 66 source and RSPAN destination sessions.
- ES ports do not support SPAN source sessions.
- You can have multiple destination ports in a SPAN session, but no more than 64 destination ports.
- You can configure two separate SPAN or RSPAN source sessions with separate or overlapping sets of SPAN source ports and VLANs. Both switched and routed ports can be configured as SPAN sources and destinations.
- SPAN sessions do not interfere with the normal operation of the switch. However, an oversubscribed SPAN destination, for example, a 10-Mbps port monitoring a 100-Mbps port, can result in dropped or lost packets.
- When RSPAN is enabled, each packet being monitored is transmitted twice, once as normal traffic and once as a monitored packet. Therefore monitoring a large number of ports or VLANs could potentially generate large amounts of network traffic.
- You can configure SPAN sessions on disabled ports; however, a SPAN session does not become active unless you enable the destination port and at least one source port or VLAN for that session.
- The switch does not support a combination of local SPAN and RSPAN in a single session. That is, an RSPAN source session cannot have a local destination port, an RSPAN destination session cannot have a local source port, and an RSPAN destination session and an RSPAN source session that are using the same RSPAN VLAN cannot run on the same switch.

**Monitored Traffic**

SPAN sessions can monitor these traffic types:

- Receive (Rx) SPAN—The goal of receive (or ingress) SPAN is to monitor as much as possible all the packets received by the source interface or VLAN before any modification or processing is performed by the switch. A copy of each packet received by the source is sent to the destination port for that SPAN session.

Packets that are modified because of routing or quality of service (QoS)—for example, modified Differentiated Services Code Point (DSCP)—are copied before modification.
Features that can cause a packet to be dropped during receive processing have no effect on ingress SPAN; the destination port receives a copy of the packet even if the actual incoming packet is dropped. These features include IP standard and extended input access control lists (ACLs), ingress QoS policing, VLAN ACLs and egress QoS policing.

- **Transmit (Tx) SPAN**—The goal of transmit (or egress) SPAN is to monitor as much as possible all the packets sent by the source interface after all modification and processing is performed by the switch. A copy of each packet sent by the source is sent to the destination port for that SPAN session. The copy is provided after the packet is modified.

  Packets that are modified because of routing—for example, with modified time-to-live (TTL), MAC-address, or QoS values—are duplicated (with the modifications) at the destination port.

  Features that can cause a packet to be dropped during transmit processing also affect the duplicated copy for SPAN. These features include IP standard and extended output ACLs and egress QoS policing.

- **Both**—In a SPAN session, you can also monitor a port or VLAN for both received and sent packets. This is the default.

The default configuration for local SPAN session ports is to send all packets untagged. SPAN also does not normally monitor bridge protocol data unit (BPDU) packets and Layer 2 protocols, such as Cisco Discovery Protocol (CDP), VLAN Trunk Protocol (VTP), Dynamic Trunking Protocol (DTP), Spanning Tree Protocol (STP), and Port Aggregation Protocol (PAgP). However, when you enter the **encapsulation replicate** keywords when configuring a destination port, these changes occur:

- Packets are sent on the destination port with the same encapsulation—untagged, IEEE 802.1Q, or Inter-Switch Link (ISL)—that they had on the source port.

- Packets of all types, including BPDU and Layer 2 protocol packets, are monitored.

Therefore, a local SPAN session with encapsulation replicate enabled can have a mixture of untagged, IEEE 802.1Q, and ISL tagged packets appear on the destination port.

Switch congestion can cause packets to be dropped at ingress source ports, egress source ports, or SPAN destination ports. In general, these characteristics are independent of one another. For example:

- A packet might be forwarded normally but dropped from monitoring due to an oversubscribed SPAN destination port.

- An ingress packet might be dropped from normal forwarding, but still appear on the SPAN destination port.

- An egress packet dropped because of switch congestion is also dropped from egress SPAN.

In some SPAN configurations, multiple copies of the same source packet are sent to the SPAN destination port. For example, a bidirectional (both Rx and Tx) SPAN session is configured for the Rx monitor on port A and Tx monitor on port B. If a packet enters the switch through port A and is switched to port B, both incoming and outgoing packets are sent to the destination port. Both packets are the same (unless a Layer-3 rewrite occurs, in which case the packets are different because of the packet modification).

---

**Source Ports**

A source port (also called a *monitored port*) is a switched or routed port that you monitor for network traffic analysis. In a local SPAN session or RSPAN source session, you can monitor source ports or VLANs for traffic in one or both directions. The switch supports any number of source ports (up to the maximum number of available ports on the switch) and any number of source VLANs (up to the maximum number of VLANs supported). However, the switch supports a maximum of two sessions (local or RSPAN) with source ports or VLANs and you cannot mix ports and VLANs in a single session.
A source port has these characteristics:

- It can be monitored in multiple SPAN sessions.
- Each source port can be configured with a direction (ingress, egress, or both) to monitor.
- It can be any port type (for example, EtherChannel, Fast Ethernet, Gigabit Ethernet, and so forth).
- For EtherChannel sources, you can monitor traffic for the entire EtherChannel or individually on a physical port as it participates in the port channel.
- It can be an access port, trunk port, routed port, or voice VLAN port.
- It cannot be an ES port.
- It cannot be a destination port.
- Source ports can be in the same or different VLANs.
- You can monitor multiple source ports in a single session.

Source VLANs

VLAN-based SPAN (VSPAN) is the monitoring of the network traffic in one or more VLANs. The SPAN or RSPAN source interface in VSPAN is a VLAN ID and traffic is monitored on all the ports for that VLAN.

VSPAN has these characteristics:

- All active ports in the source VLAN (except ES ports) are included as source ports and can be monitored in either or both directions.
- On a given port, only traffic on the monitored VLAN is sent to the destination port.
- If a destination port belongs to a source VLAN, it is excluded from the source list and is not monitored.
- If ports are added to or removed from the source VLANs, the traffic on the source VLAN received by those ports is added to or removed from the sources being monitored.
- You cannot use filter VLANs in the same session with VLAN sources.
- You can monitor only Ethernet VLANs.

VLAN Filtering

When you monitor a trunk port as a source port, by default, all VLANs active on the trunk are monitored. You can limit SPAN traffic monitoring on trunk source ports to specific VLANs by using VLAN filtering.

- VLAN filtering applies only to trunk ports or to voice VLAN ports.
- VLAN filtering applies only to port-based sessions and is not allowed in sessions with VLAN sources.
- When a VLAN filter list is specified, only those VLANs in the list are monitored on trunk ports or on voice VLAN access ports.
- SPAN traffic coming from other port types is not affected by VLAN filtering; that is, all VLANs are allowed on other ports.
- VLAN filtering affects only traffic forwarded to the destination SPAN port and does not affect the switching of normal traffic.
Destination Port

Each local SPAN session or RSPAN destination session must have a destination port (also called a monitoring port) that receives a copy of traffic from the source ports or VLANs and sends the SPAN packets to the user, usually a network analyzer.

A destination port has these characteristics:

- For a local SPAN session, the destination port must reside on the same switch as the source port. For an RSPAN session, it is located on the switch containing the RSPAN destination session. There is no destination port on a switch running only an RSPAN source session.
- When a port is configured as a SPAN destination port, the configuration overwrites the original port configuration. When the SPAN destination configuration is removed, the port reverts to its previous configuration. If a configuration change is made to the port while it is acting as a SPAN destination port, the change does not take effect until the SPAN destination configuration had been removed.
- If the port was in an EtherChannel group, it is removed from the group while it is a destination port. If it was a routed port, it is no longer a routed port.
- It can be any Ethernet physical port.
- It cannot be a secure port.
- It cannot be a source port.
- It cannot be an EtherChannel group or a VLAN.
- It can participate in only one SPAN session at a time (a destination port in one SPAN session cannot be a destination port for a second SPAN session).
- When it is active, incoming traffic is disabled. The port does not transmit any traffic except that required for the SPAN session. Incoming traffic is never learned or forwarded on a destination port.
- If ingress traffic forwarding is enabled for a network security device, the destination port forwards traffic at Layer 2.
- It does not participate in any of the Layer 2 protocols (STP, VTP, CDP, DTP, PagP).
- A destination port that belongs to a source VLAN of any SPAN session is excluded from the source list and is not monitored.
- The maximum number of destination ports in a switch is 64.

Local SPAN and RSPAN destination ports behave differently regarding VLAN tagging and encapsulation:

- For local SPAN, if the `encapsulation replicate` keywords are specified for the destination port, these packets appear with the original encapsulation (untagged, ISL, or IEEE 802.1Q). If these keywords are not specified, packets appear in the untagged format. Therefore, the output of a local SPAN session with `encapsulation replicate` enabled can contain a mixture of untagged, IEEE 802.1Q, or ISL tagged packets.
- For RSPAN, the original VLAN ID is lost because it is overwritten by the RSPAN VLAN identification. Therefore, all packets appear on the destination port as untagged.
RSPAN VLAN

The RSPAN VLAN carries SPAN traffic between RSPAN source and destination sessions. It has these special characteristics:

- All traffic in the RSPAN VLAN is always flooded.
- No MAC address learning occurs on the RSPAN VLAN.
- RSPAN VLAN traffic only flows on trunk ports.
- RSPAN VLANs must be configured in VLAN configuration mode by using the `remote-span` VLAN configuration mode command.
- STP can run on RSPAN VLAN trunks but not on SPAN destination ports.
- An RSPAN VLAN cannot be a private-VLAN primary or secondary VLAN.

For VLANs 1 to 1005 that are visible to VLAN Trunking Protocol (VTP), the VLAN ID and its associated RSPAN characteristic are propagated by VTP. If you assign an RSPAN VLAN ID in the extended VLAN range (1006 to 4094), you must manually configure all intermediate switches.

It is normal to have multiple RSPAN VLANs in a network at the same time with each RSPAN VLAN defining a network-wide RSPAN session. That is, multiple RSPAN source sessions anywhere in the network can contribute packets to the RSPAN session. It is also possible to have multiple RSPAN destination sessions throughout the network, monitoring the same RSPAN VLAN and presenting traffic to the user. The RSPAN VLAN ID separates the sessions.

SPAN and RSPAN Interaction with Other Features

SPAN interacts with these features:

- Routing—SPAN does not monitor routed traffic. VSPAN only monitors traffic that enters or exits the switch, not traffic that is routed between VLANs. For example, if a VLAN is being Rx-monitored and the switch routes traffic from another VLAN to the monitored VLAN, that traffic is not monitored and not received on the SPAN destination port.
- Spanning Tree Protocol (STP)—A destination port does not participate in STP while its SPAN or RSPAN session is active. The destination port can participate in STP after the SPAN or RSPAN session is disabled. On a source port, SPAN does not affect the STP status. STP can be active on trunk ports carrying an RSPAN VLAN.
- Cisco Discovery Protocol (CDP)—A SPAN destination port does not participate in CDP while the SPAN session is active. After the SPAN session is disabled, the port again participates in CDP.
- VLAN Trunking Protocol (VTP)—You can use VTP to prune an RSPAN VLAN between switches.
- VLAN and trunking—You can modify VLAN membership or trunk settings for source or destination ports at any time. However, changes in VLAN membership or trunk settings for a destination port do not take effect until you remove the SPAN destination configuration. Changes in VLAN membership or trunk settings for a source port immediately take effect, and the respective SPAN sessions automatically adjust accordingly.
- EtherChannel—You can configure an EtherChannel group as a source port but not as a SPAN destination port. When a group is configured as a SPAN source, the entire group is monitored.

If a physical port is added to a monitored EtherChannel group, the new port is added to the SPAN source port list. If a port is removed from a monitored EtherChannel group, it is automatically removed from the source port list.
A physical port that belongs to an EtherChannel group can be configured as a SPAN source port and still be a part of the EtherChannel. In this case, data from the physical port is monitored as it participates in the EtherChannel. However, if a physical port that belongs to an EtherChannel group is configured as a SPAN destination, it is removed from the group. After the port is removed from the SPAN session, it rejoins the EtherChannel group. Ports removed from an EtherChannel group remain members of the group, but they are in the inactive or suspended state.

If a physical port that belongs to an EtherChannel group is a destination port and the EtherChannel group is a source, the port is removed from the EtherChannel group and from the list of monitored ports.

- Multicast traffic can be monitored. For egress and ingress port monitoring, only a single unedited packet is sent to the SPAN destination port. It does not reflect the number of times the multicast packet is sent.
- A private-VLAN port cannot be a SPAN destination port.
- A secure port cannot be a SPAN destination port.
  
  For SPAN sessions, do not enable port security on ports with monitored egress when ingress forwarding is enabled on the destination port. For RSPAN source sessions, do not enable port security on any ports with monitored egress.
- An IEEE 802.1x port can be a SPAN source port. You can enable IEEE 802.1x on a port that is a SPAN destination port; however, IEEE 802.1x is disabled until the port is removed as a SPAN destination.
  
  For SPAN sessions, do not enable IEEE 802.1x on ports with monitored egress when ingress forwarding is enabled on the destination port. For RSPAN source sessions, do not enable IEEE 802.1x on any ports that are egress monitored.

**Configuring SPAN and RSPAN**

This section describes how to configure SPAN on your switch. It contains this configuration information:

- Default SPAN and RSPAN Configuration, page 28-9
- Configuring Local SPAN, page 28-10
- Configuring RSPAN, page 28-15

**Default SPAN and RSPAN Configuration**

Table 28-1 shows the default SPAN and RSPAN configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPAN state (SPAN and RSPAN)</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Source port traffic to monitor</td>
<td>Both received and sent traffic (both).</td>
</tr>
<tr>
<td>Encapsulation type (destination port)</td>
<td>Native form (untagged packets).</td>
</tr>
<tr>
<td>Ingress forwarding (destination port)</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
### Configuring Local SPAN

This section describes how to configure Local SPAN on your switch. It contains this configuration information:

- SPAN Configuration Guidelines, page 28-10
- Creating a Local SPAN Session, page 28-11
- Creating a Local SPAN Session and Configuring Ingress Traffic, page 28-13
- Specifying VLANs to Filter, page 28-14

### SPAN Configuration Guidelines

Follow these guidelines when configuring SPAN:

- You can configure a total of two local SPAN sessions or RSPAN source sessions on each switch. You can have a total of 66 SPAN sessions (local, RSPAN source, and RSPAN destination) on a switch.
- For SPAN sources, you can monitor traffic for a single port or VLAN or a series or range of ports or VLANs for each session. You cannot mix source ports and source VLANs within a single SPAN session.
- The destination port cannot be a source port; a source port cannot be a destination port.
- You cannot have two SPAN sessions using the same destination port.
- When you configure a switch port as a SPAN destination port, it is no longer a normal switch port; only monitored traffic passes through the SPAN destination port.
- Entering SPAN configuration commands does not remove previously configured SPAN parameters. You must enter the `no monitor session { session_number | all | local | remote }` global configuration command to delete configured SPAN parameters.
- For local SPAN, outgoing packets through the SPAN destination port carry the original encapsulation headers—untagged, ISL, or IEEE 802.1Q—if the `encapsulation replicate` keywords are specified. If the keywords are not specified, the packets are sent in native form. For RSPAN destination ports, outgoing packets are not tagged.
- You can configure a disabled port to be a source or destination port, but the SPAN function does not start until the destination port and at least one source port or source VLAN are enabled.
- You can limit SPAN traffic to specific VLANs by using the `filter vlan` keyword. If a trunk port is being monitored, only traffic on the VLANs specified with this keyword is monitored. By default, all VLANs are monitored on a trunk port.
- You cannot mix source VLANs and filter VLANs within a single SPAN session.
### Creating a Local SPAN Session

Beginning in privileged EXEC mode, follow these steps to create a SPAN session and specify the source (monitored) ports or VLANs and the destination (monitoring) ports:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>no monitor session {session_number</td>
</tr>
</tbody>
</table>
| **Step 3** | monitor session session_number source {interface interface-id | vlan vlan-id} [, 1-] [both | rx | tx] | Specify the SPAN session and the source port (monitored port). For session_number, the range is from 1 to 66. For interface-id, specify the source port or source VLAN to monitor. • For source interface-id, specify the source port to monitor. Valid interfaces include physical interfaces and port-channel logical interfaces (port-channel port-channel-number). Valid port channel numbers are 1 to 12. • For vlan-id, specify the source VLAN to monitor. The range is 1 to 4094 (excluding the RSPAN VLAN). **Note** A single session can include multiple sources (ports or VLANs), defined in a series of commands, but you cannot combine source ports and source VLANs in one session. (Optional) [, 1-] Specify a series or range of interfaces. Enter a space before and after the comma; enter a space before and after the hyphen. (Optional) Specify the direction of traffic to monitor. If you do not specify a traffic direction, the SPAN monitors both sent and received traffic. • both—Monitor both received and sent traffic. This is the default. • rx—Monitor received traffic. • tx—Monitor sent traffic. **Note** You can use the monitor session session_number source command multiple times to configure multiple source ports.
To delete a SPAN session, use the `no monitor session session_number` global configuration command. For `session_number`, specify the session number entered in step 3.

For `interface-id`, specify the destination port. The destination interface must be a physical port; it cannot be an EtherChannel, and it cannot be a VLAN. (Optional) `[ ]` Specify a series or range of interfaces. Enter a space before and after the comma; enter a space before and after the hyphen. (Optional) Enter `encapsulation replicate` to specify that the destination interface replicates the source interface encapsulation method. If not selected, the default is to send packets in native form (untagged).

To remove a source or destination port or VLAN from the SPAN session, use the `no monitor session session_number source [interface interface-id | vlan vlan-id]` global configuration command or the `no monitor session session_number destination interface interface-id` global configuration command. For destination interfaces, the `encapsulation replicate` keywords are ignored with the `no` form of the command. For local SPAN, you must use the same session number for the source and destination interfaces.

This example shows how to set up local SPAN session 1, for monitoring source port traffic to a destination port. First, any existing SPAN configuration for session 1 is deleted, and then bidirectional traffic is mirrored from source Gigabit Ethernet port 1 to destination Gigabit Ethernet port 2, retaining the encapsulation method.

```
Switch(config)# no monitor session 1
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1
Switch(config)# monitor session 1 destination interface gigabitethernet1/0/2
encapsulation replicate
Switch(config)# end
```

This example shows how to remove a port as a SPAN source for SPAN session 1:

```
Switch(config)# no monitor session 1 source interface gigabitethernet1/0/1
Switch(config)# end
```

This example shows how to disable monitoring received traffic on a port that was configured for bidirectional monitoring:

```
Switch(config)# no monitor session 1 source interface gigabitethernet1/0/1 rx
```

Traffic received on port 1 is not monitored, but traffic sent from this port continues to be monitored.
This example shows how to remove any existing configuration on SPAN session 2, configure SPAN session 2 to monitor received traffic on all ports belonging to VLANs 1 through 3, and send it to a destination interface. The configuration is then modified to also monitor all traffic on all ports belonging to VLAN 10.

```bash
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source vlan 1 - 3 rx
Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2
Switch(config)# monitor session 2 source vlan 10
Switch(config)# end
```

## Creating a Local SPAN Session and Configuring Ingress Traffic

Beginning in privileged EXEC mode, follow these steps to create a SPAN session, to specify the source ports or VLANs and the destination ports, and to enable incoming traffic on the destination port for a network security device (such as a Cisco IDS Sensor Appliance).

For details about the keywords not related to ingress traffic, see the “Creating a Local SPAN Session” section on page 28-11.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>no monitor session {session_number</td>
<td>all</td>
</tr>
<tr>
<td>Step 3</td>
<td>monitor session session_number source {interface interface-id</td>
<td>vlan vlan-id} [,</td>
</tr>
</tbody>
</table>
| Step 4 | monitor session session_number destination {interface interface-id [, | -] [encapsulation replicate] [ingress [dot1q vlan vlan-id | isl | untagged vlan vlan-id | vlan vlan-id]]} | Specify the SPAN session, the destination port, the packet encapsulation, and the ingress VLAN and encapsulation. For session_number, specify the session number entered in Step 3. For interface-id, specify the destination port. The destination interface must be a physical port; it cannot be an EtherChannel, and it cannot be a VLAN. (Optional) [, | -] Specify a series or range of interfaces. Enter a space before and after the comma or hyphen. (Optional) Enter encapsulation replicate to specify that the destination interface replicates the source interface encapsulation method. If not selected, the default is to send packets in native form (untagged).

Enter ingress with keywords to enable ingress traffic forwarding on the destination port and specify the encapsulation type:

- **dot1q vlan vlan-id**—Forward ingress packets with IEEE 802.1Q encapsulation with the specified VLAN as the default VLAN.
- **isl**—Forward ingress packets with ISL encapsulation.
- **untagged vlan vlan-id or vlan vlan-id**—Forward ingress packets with untagged encapsulation type with the specified VLAN as the default VLAN.

| Step 5 | end | Return to privileged EXEC mode. |

---

Ol-9644-09

Catalyst 3750 Metro Switch Software Configuration Guide

28-13
Chapter 28      Configuring SPAN and RSPAN

Configuration

To delete a SPAN session, use the `no monitor session session_number` global configuration command. To remove a source or destination port or VLAN from the SPAN session, use the `no monitor session session_number source {interface interface-id | vlan vlan-id}` global configuration command or the `no monitor session session_number destination interface interface-id` global configuration command. For destination interfaces, the encapsulation and ingress options are ignored with the `no` form of the command.

This example shows how to remove any existing configuration on SPAN session 2, configure SPAN session 2 to monitor received traffic on Gigabit Ethernet source port 1, and send it to destination Gigabit Ethernet port 2 with the same egress encapsulation type as the source port, and enable ingress forwarding with IEEE 802.1Q encapsulation and VLAN 6 as the default ingress VLAN.

```
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source gigabitethernet1/0/1 rx
Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2 encapsulation replicate ingress dot1q vlan 6
Switch(config)# end
```

Specifying VLANs to Filter

Beginning in privileged EXEC mode, follow these steps to limit SPAN source traffic to specific VLANs:

```
Step 1 configure terminal
Step 2 no monitor session {session_number | all | local | remote}
Step 3 monitor session session_number source interface interface-id
Step 4 monitor session session_number filter vlan vlan-id [ , 1 - ]
```

Command                  Purpose
---                      ---
configure terminal       Enter global configuration mode.
no monitor session {session_number | all | local | remote} Remove any existing SPAN configuration for the session.
                        For `session_number`, the range is from 1 to 66.
                        Specify `all` to remove all SPAN sessions, `local` to remove all local
                        sessions, or `remote` to remove all remote SPAN sessions.
monitor session session_number source interface interface-id Specify the characteristics of the source port (monitored port) and
                        SPAN session.
                        For `session_number`, the range is from 1 to 66.
                        For `interface-id`, specify the source port to monitor. The interface
                        specified must already be configured as a trunk port.
monitor session session_number filter vlan vlan-id [ , 1 - ] Limit the SPAN source traffic to specific VLANs.
                        For `session_number`, enter the session number specified in Step 3.
                        For `vlan-id`, the range is 1 to 4094.
                        (Optional) Use a comma (,) to specify a series of VLANs, or use a
                        hyphen (-) to specify a range of VLANs. Enter a space before and after
                        the comma; enter a space before and after the hyphen.
To monitor all VLANs on the trunk port, use the `no monitor session session_number filter` global configuration command.

This example shows how to remove any existing configuration on SPAN session 2, configure SPAN session 2 to monitor traffic received on Gigabit Ethernet trunk port 2, and send traffic for only VLANs 1 through 5 and 9 to destination Gigabit Ethernet port 1.

```
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source interface gigabitethernet1/0/2 rx
Switch(config)# monitor session 2 filter vlan 1 - 5, 9
Switch(config)# monitor session 2 destination interface gigabitethernet1/0/1
Switch(config)# end
```

### Configuring RSPAN

This section describes how to configure RSPAN on your switch. It contains this configuration information:

- **RSPAN Configuration Guidelines**, page 28-16
- **Configuring a VLAN as an RSPAN VLAN**, page 28-16
- **Creating an RSPAN Source Session**, page 28-17
- **Creating an RSPAN Destination Session**, page 28-19
- **Specifying VLANs to Filter**, page 28-22
RSPAN Configuration Guidelines

Follow these guidelines when configuring RSPAN:

- All the items in the “SPAN Configuration Guidelines” section on page 28-10 apply to RSPAN.
- As RSPAN VLANs have special properties, you should reserve a few VLANs across your network for use as RSPAN VLANs; do not assign access ports to these VLANs.
- You can apply an output access control list (ACL) to RSPAN traffic to selectively filter or monitor specific packets. Specify these ACLs on the RSPAN VLAN in the RSPAN source switches.
- For RSPAN configuration, you can distribute the source ports and the destination ports across multiple switches in your network.
- RSPAN does not support BPDU packet monitoring or other Layer 2 switch protocols.
- The RSPAN VLAN is configured only on trunk ports and not on access ports. To avoid unwanted traffic in RSPAN VLANs, make sure that the VLAN remote-span feature is supported in all the participating switches.
- Access ports (including voice VLAN ports) on the RSPAN VLAN are put in the inactive state.
- RSPAN VLANs are included as sources for port-based RSPAN sessions when source trunk ports have active RSPAN VLANs. RSPAN VLANs can also be sources in SPAN sessions. However, since the switch does not monitor spanned traffic, it does not support egress spanning of packets on any RSPAN VLAN identified as the destination of an RSPAN source session on the switch.
- You can configure any VLAN as an RSPAN VLAN as long as these conditions are met:
  - The same RSPAN VLAN is used for an RSPAN session in all the switches.
  - All participating switches support RSPAN.
- We recommend that you configure an RSPAN VLAN before you configure an RSPAN source or a destination session.
- If you enable VTP and VTP pruning, RSPAN traffic is pruned in the trunks to prevent the unwanted flooding of RSPAN traffic across the network for VLAN IDs that are lower than 1005.

Configuring a VLAN as an RSPAN VLAN

First create a new VLAN to be the RSPAN VLAN for the RSPAN session. You must create the RSPAN VLAN in all switches that will participate in RSPAN. If the RSPAN VLAN-ID is in the normal range (lower than 1005) and VTP is enabled in the network, you can create the RSPAN VLAN in one switch, and VTP propagates it to the other switches in the VTP domain. For extended-range VLANs (greater than 1005), you must configure RSPAN VLAN on both source and destination switches and any intermediate switches.

Use VTP pruning to get an efficient flow of RSPAN traffic, or manually delete the RSPAN VLAN from all trunks that do not need to carry the RSPAN traffic.
Beginning in privileged EXEC mode, follow these steps to create an RSPAN VLAN:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>vlan vlan-id</td>
<td>Enter a VLAN ID to create a VLAN, or enter the VLAN ID of an existing VLAN, and enter VLAN configuration mode. The range is from 2 to 1001 and from 1006 to 4094.</td>
</tr>
<tr>
<td></td>
<td>remote-span</td>
<td>Configure the VLAN as an RSPAN VLAN.</td>
</tr>
<tr>
<td></td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save the configuration in the configuration file.</td>
</tr>
</tbody>
</table>

To remove the remote SPAN characteristic from a VLAN and convert it back to a normal VLAN, use the `no remote-span VLAN` configuration command.

This example shows how to create RSPAN VLAN 901.

```plaintext
Switch(config)# vlan 901
Switch(config-vlan)# remote span
Switch(config-vlan)# end
```

### Creating an RSPAN Source Session

Beginning in privileged EXEC mode, follow these steps to start an RSPAN source session and to specify the monitored source and the destination RSPAN VLAN:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>no monitor session {session_number</td>
<td>all</td>
</tr>
</tbody>
</table>
Chapter 28 Configuring SPAN and RSPAN

Configuring SPAN and RSPAN

To delete a SPAN session, use the no monitor session session_number global configuration command.

To remove a source port or VLAN from the SPAN session, use the no monitor session session_number source {interface interface-id | vlan vlan-id} [ , | - ] [both | rx | tx] global configuration command. To remove the RSPAN VLAN from the session, use the no monitor session session_number destination remote vlan vlan-id.

This example shows how to remove any existing RSPAN configuration for session 1, configure RSPAN session 1 to monitor multiple source interfaces, and configure the destination as RSPAN VLAN 901.

Switch(config)# no monitor session 1
Switch(config)# monitor session 1 source interface fastethernet1/0/10 tx
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1 rx
Switch(config)# monitor session 1 source interface gigabitethernet1/0/2
Switch(config)# monitor session 1 source interface port-channel 12
Switch(config)# monitor session 1 destination remote vlan 901
Switch(config)# end

Step 3

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| monitor session session_number source {interface interface-id | vlan vlan-id} [ , | - ] [both | rx | tx] | Specify the RSPAN session and the source port (monitored port). For session_number, the range is from 1 to 66. Enter a source port or source VLAN for the RSPAN session:  
  - For interface-id, specify the source port to monitor. Valid interfaces include physical interfaces and port-channel logical interfaces (port-channel port-channel-number). Valid port channel numbers are 1 to 12.  
  - For vlan-id, specify the source VLAN to monitor. The range is 1 to 4094 (excluding the RSPAN VLAN).  
  Note: A single session can include multiple sources (ports or VLANs), defined in a series of commands, but you cannot combine source ports and source VLANs in one session.  
  (Optional) [ , | - ] Specify a series or range of interfaces. Enter a space before and after the comma; enter a space before and after the hyphen.  
  (Optional) Specify the direction of traffic to monitor. If you do not specify a traffic direction, the source interface sends both sent and received traffic.  
    - both—Monitor both received and sent traffic.  
    - rx—Monitor received traffic.  
    - tx—Monitor sent traffic. |

Step 4

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>monitor session session_number destination remote vlan vlan-id</td>
<td>Specify the RSPAN session and the destination RSPAN VLAN. For session_number, enter the number defined in Step 3. For vlan-id, specify the source RSPAN VLAN to monitor.</td>
</tr>
</tbody>
</table>

Step 5

end

Step 6

show monitor [session session_number]
show running-config

Step 7

copy running-config startup-config

(Optional) Save the configuration in the configuration file.
## Creating an RSPAN Destination Session

You configure the RSPAN destination session on a different switch; that is, not the switch on which the source session was configured.

Beginning in privileged EXEC mode, follow these steps to define the RSPAN VLAN on that switch, to create an RSPAN destination session, and to specify the source RSPAN VLAN and the destination port:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
</tbody>
</table>
| 2    | vlan vlan-id | Enter the VLAN ID of the RSPAN VLAN created from the source switch, and enter VLAN configuration mode.  
      |         | **Note** If both switches are participating in VTP and the RSPAN VLAN ID is from 2 to 1005, Steps 2 through 4 are not required because the RSPAN VLAN ID is propagated through the VTP network. |
| 3    | remote-span | Identify the VLAN as the RSPAN VLAN. |
| 4    | exit | Return to global configuration mode. |
| 5    | no monitor session {session_number | Remove any existing RSPAN configuration for the session.  
      |  all | For *session_number*, the range is from 1 to 66.  
      | local | Specify all to remove all RSPAN sessions, local to remove all local sessions, or remote to remove all remote SPAN sessions. |
|      | remote} | |
| 6    | monitor session session_number source remote vlan vlan-id | Specify the RSPAN session and the source RSPAN VLAN.  
      |         | For *session_number*, the range is from 1 to 66.  
      |         | For *vlan-id*, specify the source RSPAN VLAN to monitor. |
| 7    | monitor session session_number destination interface interface-id | Specify the RSPAN session and the destination interface.  
      |         | For *session_number*, enter the number defined in Step 6.  
      |         | **Note** In an RSPAN destination session, you must use the same session number for the source RSPAN VLAN and the destination port.  
      |         | For *interface-id*, specify the destination interface. The destination interface must be a physical interface.  
      |         | **Note** Though visible in the command-line help string, encapsulation replicate is not supported for RSPAN. The original VLAN ID is overwritten by the RSPAN VLAN ID, and all packets appear on the destination port as untagged. |
| 8    | end | Return to privileged EXEC mode. |
| 9    | show monitor [session session_number] | Verify the configuration. |
| 10   | show running-config | |
|      | copy running-config startup-config | (Optional) Save the configuration in the configuration file. |
To delete a SPAN session, use the `no monitor session session_number` global configuration command. To remove a destination port from the SPAN session, use the `no monitor session session_number destination interface interface-id` global configuration command. To remove the RSPAN VLAN from the session, use the `no monitor session session_number source remote vlan vlan-id`.

This example shows how to configure VLAN 901 as the source remote VLAN and Gigabit Ethernet port 2 as the destination interface:

```
Switch(config)# monitor session 1 source remote vlan 901
Switch(config)# monitor session 1 destination interface gigabitethernet1/0/2
Switch(config)# end
```

**Creating an RSPAN Destination Session and Configuring Incoming Traffic**

Beginning in privileged EXEC mode, follow these steps to create an RSPAN destination session, to specify the source RSPAN VLAN and the destination port, and to enable incoming traffic on the destination port for a network security device (such as a Cisco IDS Sensor Appliance).

For details about the keywords not related to ingress traffic, see the “Creating an RSPAN Destination Session” section on page 28-19. This procedure assumes the RSPAN VLAN has already been configured.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code> Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>`no monitor session {session_number</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>monitor session session_number source remote vlan vlan-id</code> Specify the RSPAN session and the source RSPAN VLAN. For <code>session_number</code>, the range is 1 to 66. For <code>vlan-id</code>, specify the source RSPAN VLAN to monitor.</td>
</tr>
</tbody>
</table>
To delete an RSPAN session, use the `no monitor session session_number` global configuration command. To remove a destination port from the RSPAN session, use the `no monitor session session_number destination interface-id` global configuration command. The ingress options are ignored with the `no` form of the command.

This example shows how to configure VLAN 901 as the source remote VLAN in RSPAN session 2, to configure Gigabit Ethernet source port 2 as the destination interface, and to enable ingress forwarding on the interface with VLAN 6 as the default receiving VLAN.

```
Switch(config)# monitor session 2 source remote vlan 901
Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2 ingress vlan 6
Switch(config)# end
```
Specifying VLANs to Filter

Beginning in privileged EXEC mode, follow these steps to configure the RSPAN source session to limit RSPAN source traffic to specific VLANs:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>no monitor session {session_number</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>monitor session session_number source interface interface-id</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>monitor session session_number filter vlan vlan-id [,</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>monitor session session_number destination remote vlan vlan-id</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>show monitor {session session_number}</td>
</tr>
<tr>
<td></td>
<td>show running-config</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To monitor all VLANs on the trunk port, use the no monitor session session_number filter vlan global configuration command.

This example shows how to remove any existing configuration on RSPAN session 2, configure RSPAN session 2 to monitor traffic received on a trunk port, and send traffic for only VLANs 1 through 5 and 9 to destination RSPAN VLAN 902.

```
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source interface gigabitethernet1/0/2 rx
Switch(config)# monitor session 2 filter vlan 1 - 5, 9
Switch(config)# monitor session 2 destination remote vlan 902
Switch(config)# end
```
Displaying SPAN and RSPAN Status

To display the current SPAN or RSPAN configuration, use the `show monitor` user EXEC command. You can also use the `show running-config` privileged EXEC command to display configured SPAN or RSPAN sessions.
Configuring RMON

This chapter describes how to configure Remote Network Monitoring (RMON) on the Catalyst 3750 Metro switch.

RMON is a standard monitoring specification that defines a set of statistics and functions that can be exchanged between RMON-compliant console systems and network probes. RMON provides you with comprehensive network-fault diagnosis, planning, and performance-tuning information.

Note

For complete syntax and usage information for the commands used in this chapter, see the “System Management Commands” section in the Cisco IOS Configuration Fundamentals Command Reference, Release 12.2.

This chapter consists of these sections:

- Understanding RMON, page 29-1
- Configuring RMON, page 29-3
- Displaying RMON Status, page 29-6

Understanding RMON

RMON is an Internet Engineering Task Force (IETF) standard monitoring specification that allows various network agents and console systems to exchange network monitoring data. You can use the RMON feature with the Simple Network Management Protocol (SNMP) agent in the switch to monitor all the traffic flowing among switches on all connected LAN segments.
The switch supports these RMON groups (defined in RFC 1757):

- **Statistics (RMON group 1)**—Collects Ethernet, Fast Ethernet, and Gigabit Ethernet statistics on a port.
- **History (RMON group 2)**—Collects a history group of statistics on Ethernet, Fast Ethernet, and Gigabit Ethernet ports for a specified polling interval.
- **Alarm (RMON group 3)**—Monitors a specific MIB object for a specified interval, triggers an alarm at a specified value (rising threshold), and resets 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.
- **Event (RMON group 9)**—Specifies 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.

Because switches supported by this software release use hardware counters for RMON data processing, the monitoring is more efficient, and little processing power is required.

**Note**

64-bit counters are not supported for RMON alarms.
Configuring RMON

These sections describe how to configure RMON on your switch:

- Default RMON Configuration, page 29-3
- Configuring RMON Alarms and Events, page 29-3 (required)
- Collecting Group History Statistics on an Interface, page 29-5 (optional)
- Collecting Group Ethernet Statistics on an Interface, page 29-6 (optional)

Default RMON Configuration

RMON is disabled by default; no alarms or events are configured.

Configuring RMON Alarms and Events

You can configure your switch for RMON by using the command-line interface (CLI) or an SNMP-compatible network management station. We recommend that you use a generic RMON console application on the network management station (NMS) to take advantage of RMON’s network management capabilities. You must also configure SNMP on the switch to access RMON MIB objects. For more information, see Chapter 31, “Configuring SNMP.”

Note

64-bit counters are not supported for RMON alarms.

Beginning in privileged EXEC mode, follow these steps to enable RMON alarms and events. This procedure is required.
Chapter 29 Configuring RMON

Configuring RMON

To disable an alarm, use the no rmon alarm number global configuration command on each alarm you configured. You cannot disable at once all the alarms that you configured. To disable an event, use the no rmon event number global configuration command. To learn more about alarms and events and how they interact with each other, see RFC 1757.

Command Purpose

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>rmon alarm number variable interval [absolute</td>
<td>Set an alarm on a MIB object.</td>
</tr>
<tr>
<td>delta]</td>
<td>For number, specify the alarm number. The range is 1 to 65535.</td>
</tr>
<tr>
<td>rising-threshold value [event-number]</td>
<td>For variable, specify the MIB object to monitor.</td>
</tr>
<tr>
<td>falling-threshold value [event-number]</td>
<td>For interval, specify the time in seconds the alarm monitors the MIB variable. The range is 1 to 4294967295 seconds.</td>
</tr>
<tr>
<td>[owner string]</td>
<td>Specify the absolute keyword to test each MIB variable directly. Specify the delta keyword to test the change between samples of a MIB variable.</td>
</tr>
<tr>
<td>rmon event number [description string] [log] [owner string]</td>
<td>Add an event in the RMON event table that is associated with an RMON event number.</td>
</tr>
<tr>
<td>[trap community]</td>
<td>For number, assign an event number. The range is 1 to 65535.</td>
</tr>
<tr>
<td></td>
<td>(Optional) For description string, specify a description of the event.</td>
</tr>
<tr>
<td></td>
<td>(Optional) Use the log keyword to generate an RMON log entry when the event is triggered.</td>
</tr>
<tr>
<td></td>
<td>(Optional) For owner string, specify the owner of this event.</td>
</tr>
<tr>
<td></td>
<td>(Optional) For trap community, enter the SNMP community string used for this trap.</td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
You can set an alarm on any MIB object. The following example configures RMON alarm number 10 by using the `rmon alarm` command. The alarm monitors the MIB variable `ifEntry.20.1` once every 20 seconds until the alarm is disabled and checks the change in the variable’s rise or fall. If the `ifEntry.20.1` value shows a MIB counter increase of 15 or more, such as from 100000 to 100015, the alarm is triggered. The alarm in turn triggers event number 1, which is configured with the `rmon event` command. Possible events can include a log entry or an SNMP trap. If the `ifEntry.20.1` value changes by 0, the alarm is reset and can be triggered again.

```
Switch(config)# rmon alarm 10 ifEntry.20.1 20 delta rising-threshold 15 1 falling-threshold 0 owner jjohnson
```

The following example creates RMON event number 1 by using the `rmon event` command. The event is defined as `High ifOutErrors` and generates a log entry when the event is triggered by the alarm. The user `jjones` owns the row that is created in the event table by this command. This example also generates an SNMP trap when the event is triggered.

```
Switch(config)# rmon event 1 log trap eventtrap description "High ifOutErrors" owner jjones
```

**Collecting Group History Statistics on an Interface**

You must first configure RMON alarms and events to display collection information.

Beginning in privileged EXEC mode, follow these steps to collect group history statistics on an interface. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
</tbody>
</table>
| Step 3  | rmon collection history index [buckets bucket-number] [interval seconds] [owner ownername] | Enable history collection for the specified number of buckets and time period.  
   - For `index`, identify the RMON group of statistics. The range is 1 to 65535.  
   - (Optional) For `buckets bucket-number`, specify the maximum number of buckets desired for the RMON collection history group of statistics. The range is 1 to 65535. The default is 50 buckets.  
   - (Optional) For `interval seconds`, specify the number of seconds in each polling cycle. The range is 1 to 3600. The default is 1800 seconds.  
   - (Optional) For `owner ownername`, enter the name of the owner of the RMON group of statistics. |
| Step 4  | end | Return to privileged EXEC mode. |
| Step 5  | show running-config | Verify your entries. |
| Step 6  | show rmon history | Display the contents of the switch history table. |
| Step 7  | copy running-config startup-config | (Optional) Save your entries in the configuration file. |
To disable history collection, use the `no rmon collection history index` interface configuration command.

## Collecting Group Ethernet Statistics on an Interface

Beginning in privileged EXEC mode, follow these steps to collect group Ethernet statistics on an interface. This procedure is optional.

```plaintext
<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>rmon collection stats index [owner ownername]</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
</tr>
<tr>
<td>Step 5</td>
<td>show running-config</td>
</tr>
<tr>
<td>Step 6</td>
<td>show rmon statistics</td>
</tr>
<tr>
<td>Step 7</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>
```

To disable the collection of group Ethernet statistics, use the `no rmon collection stats index` interface configuration command.

This example shows how to collect RMON statistics for the owner `root`:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# rmon collection stats 2 owner root
```

## Displaying RMON Status

To display the RMON status, use one or more of the privileged EXEC commands in Table 29-1:

### Table 29-1 Commands for Displaying RMON Status

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show rmon</td>
<td>Displays general RMON statistics.</td>
</tr>
<tr>
<td>show rmon alarms</td>
<td>Displays the RMON alarm table.</td>
</tr>
<tr>
<td>show rmon events</td>
<td>Displays the RMON event table.</td>
</tr>
<tr>
<td>show rmon history</td>
<td>Displays the RMON history table.</td>
</tr>
<tr>
<td>show rmon statistics</td>
<td>Displays the RMON statistics table.</td>
</tr>
</tbody>
</table>

For information about the fields in these displays, see the “System Management Commands” section in the *Cisco IOS Configuration Fundamentals Command Reference, Release 12.2*. 
Configuring System Message Logging

This chapter describes how to configure system message logging on the Catalyst 3750 Metro switch.

Note
For complete syntax and usage information for the commands used in this chapter, see the Cisco IOS Configuration Fundamentals Command Reference, Release 12.2.

This chapter consists of these sections:
- Understanding System Message Logging, page 30-1
- Configuring System Message Logging, page 30-2
- Displaying the Logging Configuration, page 30-13

Caution
Logging messages to the console at a high rate can cause high CPU utilization and adversely affect how the switch operates.

Understanding System Message Logging

By default, a switch sends the output from system messages and debug privileged EXEC commands to a logging process. The logging process controls the distribution of logging messages to various destinations, such as the logging buffer, terminal lines, or a UNIX syslog server, depending on your configuration. The process also sends messages to the console.

Note
The syslog format is compatible with 4.3 BSD UNIX.

When the logging process is disabled, messages are sent only to the console. The messages are sent as they are generated, so message and debug output are interspersed with prompts or output from other commands. Messages are displayed on the console after the process that generated them has finished.

You can set the severity level of the messages to control the type of messages displayed on the consoles and each of the destinations. You can time-stamp log messages or set the syslog source address to enhance real-time debugging and management. For information on possible messages, see the system message guide for this release.

You can access logged system messages by using the switch command-line interface (CLI) or by saving them to a properly configured syslog server. The switch software saves syslog messages in an internal buffer on the switch. If the switch fails, the log is lost unless you had saved it to flash memory.
You can remotely monitor system messages by viewing the logs on a syslog server or by accessing the switch through Telnet or through the console port.

## Configuring System Message Logging

These sections describe how to configure system message logging:

- System Log Message Format, page 30-2
- Default System Message Logging Configuration, page 30-3
- Disabling Message Logging, page 30-4 (optional)
- Setting the Message Display Destination Device, page 30-4 (optional)
- Synchronizing Log Messages, page 30-5 (optional)
- Enabling and Disabling Timestamps on Log Messages, page 30-7 (optional)
- Enabling and Disabling Sequence Numbers in Log Messages, page 30-7 (optional)
- Defining the Message Severity Level, page 30-8 (optional)
- Limiting Syslog Messages Sent to the History Table and to SNMP, page 30-9 (optional)
- Enabling the Configuration-Change Logger, page 30-10 (optional)
- Configuring UNIX Syslog Servers, page 30-11 (optional)

### System Log Message Format

System log messages can contain up to 80 characters and a percent sign (%), which follows the optional sequence number or time-stamp information, if configured. Messages are displayed in this format:

```
seq no:timestamp: %facility-severity-MNEMONIC:description
```

The part of the message preceding the percent sign depends on the setting of the `service sequence-numbers`, `service timestamps log [datetime | log] [localtime] [msec] [show-timezone]`, or `service timestamps log uptime` global configuration command.

Table 30-1 describes the elements of syslog messages.

<table>
<thead>
<tr>
<th>Table 30-1 System Log Message Elements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Element</strong></td>
</tr>
<tr>
<td><code>seq no:</code></td>
</tr>
<tr>
<td><em>timestamp formats:</em> <code>mm/dd hh:mm:ss</code> or <code>hh:mm:ss</code> (short uptime) or <code>d h</code> (long uptime)</td>
</tr>
</tbody>
</table>
This example shows a partial switch system message:

00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/2, changed state to up
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to down

*Mar  1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
18:47:02: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
*Mar  1 18:48:50.483 UTC: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)

This example shows a partial switch system message:

Table 30-1  System Log Message Elements (continued)

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>facility</td>
<td>The facility to which the message refers (for example, SNMP, SYS, and so forth). For a list of supported facilities, see Table 30-4 on page 30-13.</td>
</tr>
<tr>
<td>severity</td>
<td>Single-digit code from 0 to 7 that is the severity of the message. For a description of the severity levels, see Table 30-3 on page 30-9.</td>
</tr>
<tr>
<td>MNEMONIC</td>
<td>Text string that uniquely describes the message.</td>
</tr>
<tr>
<td>description</td>
<td>Text string containing detailed information about the event being reported.</td>
</tr>
</tbody>
</table>

Table 30-2  Default System Message Logging Configuration

Table 30-2 shows the default system message logging configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>System message logging to the console</td>
<td>Enabled.</td>
</tr>
<tr>
<td>Console severity</td>
<td>Debugging (and numerically lower levels; see Table 30-3 on page 30-9).</td>
</tr>
<tr>
<td>Logging file configuration</td>
<td>No filename specified.</td>
</tr>
<tr>
<td>Logging buffer size</td>
<td>4096 bytes.</td>
</tr>
<tr>
<td>Logging history size</td>
<td>1 message.</td>
</tr>
<tr>
<td>Timestamps</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Synchronous logging</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Logging server</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Syslog server IP address</td>
<td>None configured.</td>
</tr>
<tr>
<td>Server facility</td>
<td>Local7 (see Table 30-4 on page 30-13).</td>
</tr>
<tr>
<td>Server severity</td>
<td>Informational (and numerically lower levels; see Table 30-3 on page 30-9).</td>
</tr>
</tbody>
</table>
Disabling Message Logging

Message logging is enabled by default. It must be enabled to send messages to any destination other than the console. When enabled, log messages are sent to a logging process, which logs messages to designated locations asynchronously to the processes that generated the messages.

Beginning in privileged EXEC mode, follow these steps to disable message logging. This procedure is optional.

### Command | Purpose
--- | ---
**Step 1** | configure terminal <br>Enter global configuration mode.  
**Step 2** | no logging on  
Disable message logging.  
**Step 3** | end  
Return to privileged EXEC mode.  
**Step 4** | show running-config  
Verify your entries.  
**Step 5** | show logging  
or  
**Step 5** | copy running-config startup-config  
(Optional) Save your entries in the configuration file.  

Disabling the logging process can slow down the switch because a process must wait until the messages are written to the console before continuing. When the logging process is disabled, messages are displayed on the console as soon as they are produced, often appearing in the middle of command output.

The `logging synchronous` global configuration command also affects the display of messages to the console. When this command is enabled, messages appear only after you press Return. For more information, see the “Synchronizing Log Messages” section on page 30-5.

To re-enable message logging after it has been disabled, use the `logging on` global configuration command.

Setting the Message Display Destination Device

If message logging is enabled, you can send messages to specific locations in addition to the console. Beginning in privileged EXEC mode, use one or more of the following commands to specify the locations that receive messages. This procedure is optional.

### Command | Purpose
--- | ---
**Step 1** | configure terminal  
Enter global configuration mode.  
**Step 2** | logging buffered [size]  
Log messages to an internal buffer on the switch. The default buffer size is 4096. The range is 4096 to 2147483647 bytes.  
If the switch, the log file is lost unless you previously saved it to flash memory. See Step 4.  
**Note** | Do not make the buffer size too large because the switch could run out of memory for other tasks. Use the `show memory` privileged EXEC command to view the free processor memory on the switch. However, this value is the maximum available, and the buffer size should not be set to this amount.  

Chapter 30 Configuring System Message Logging

Configuring System Message Logging

The `logging buffered` global configuration command copies logging messages to an internal buffer. The buffer is circular, so newer messages overwrite older messages after the buffer is full. To display the messages that are logged in the buffer, use the `show logging` privileged EXEC command. The first message displayed is the oldest message in the buffer. To clear the contents of the buffer, use the `clear logging` privileged EXEC command.

To disable logging to the console, use the `no logging console` global configuration command. To disable logging to a file, use the `no logging file [severity-level-number | type]` global configuration command.

### Synchronizing Log Messages

You can synchronize unsolicited messages and `debug` privileged EXEC command output with solicited device output and prompts for a specific console port line or virtual terminal line. You can identify the types of messages to be output asynchronously based on the level of severity. You can also configure the maximum number of buffers for storing asynchronous messages for the terminal after which messages are dropped.
When synchronous logging of unsolicited messages and `debug` command output is enabled, unsolicited device output appears on the console or printed after solicited device output appears or printed. Unsolicited messages and `debug` command output appears on the console after the prompt for user input is returned. Therefore, unsolicited messages and `debug` command output are not interspersed with solicited device output and prompts. After the unsolicited messages are displayed, the console again displays the user prompt.

Beginning in privileged EXEC mode, follow these steps to configure synchronous logging. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>`line [console</td>
<td>vty] line-number [ending-line-number]`</td>
</tr>
<tr>
<td></td>
<td>• Use the <code>console</code> keyword for configurations that occur through the switch console port.</td>
</tr>
<tr>
<td></td>
<td>• Use the <code>line vty line-number</code> command to specify which vty lines are to have synchronous logging enabled. You use a vty connection for configurations that occur through a Telnet session. The range of line numbers is from 0 to 15.</td>
</tr>
<tr>
<td></td>
<td>You can change the setting of all 16 vty lines at once by entering: <code>line vty 0 15</code></td>
</tr>
<tr>
<td></td>
<td>Or you can change the setting of the single vty line being used for your current connection. For example, to change the setting for vty line 2, enter: <code>line vty 2</code></td>
</tr>
<tr>
<td></td>
<td>When you enter this command, the mode changes to line configuration.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>`logging synchronous [level [severity-level</td>
<td>Enable synchronous logging of messages.</td>
</tr>
<tr>
<td>all]</td>
<td>limit number-of-buffers]`</td>
</tr>
<tr>
<td></td>
<td>• (Optional) Specifying <code>level all</code> means that all messages are printed asynchronously regardless of the severity level.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) For <code>limit number-of-buffers</code>, specify the number of buffers to be queued for the terminal after which new messages are dropped. The range is 0 to 2147483647. The default is 20.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td><code>show running-config</code></td>
<td>Verify your entries.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable synchronization of unsolicited messages and debug output, use the `no logging synchronous [level severity-level | all] [limit number-of-buffers]` line configuration command.
Enabling and Disabling Timestamps on Log Messages

By default, log messages are not time-stamped.

Beginning in privileged EXEC mode, follow these steps to enable time-stamping of log messages. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 service timestamps log uptime</td>
<td>Enable log time-stamps.</td>
</tr>
<tr>
<td></td>
<td>The first command enables time-stamps on log messages, showing the time since the system was rebooted.</td>
</tr>
<tr>
<td>or</td>
<td>The second command enables time-stamps on log messages. Depending on the options selected, the timestamp can include the date, time in milliseconds relative to the local time zone, and the time zone name.</td>
</tr>
<tr>
<td>service timestamps log datetime [msec] [localtime] [show-timezone]</td>
<td></td>
</tr>
<tr>
<td>Step 3 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4 show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 5 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable time-stamps for both debug and log messages, use the no service timestamps global configuration command.

This example shows part of a logging display with the service timestamps log datetime global configuration command enabled:

*Mar 1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)

This example shows part of a logging display with the service timestamps log uptime global configuration command enabled:

00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up

Enabling and Disabling Sequence Numbers in Log Messages

Because there is a chance that more than one log message can have the same timestamp, you can display messages with sequence numbers so that you can unambiguously refer to a single message. By default, sequence numbers in log messages are not displayed.

Beginning in privileged EXEC mode, follow these steps to enable sequence numbers in log messages. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 service sequence-numbers</td>
<td>Enable sequence numbers.</td>
</tr>
<tr>
<td>Step 3 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4 show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 5 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
To disable sequence numbers, use the **no service sequence-numbers** global configuration command. This example shows part of a logging display with sequence numbers enabled:

000019: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)

### Defining the Message Severity Level

You can limit messages displayed to the selected device by specifying the severity level of the message, which are described in Table 30-3.

Beginning in privileged EXEC mode, follow these steps to define the message severity level. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong> Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>logging console level</strong> Limit messages logged to the console. By default, the console receives debugging messages and numerically lower levels (see Table 30-3 on page 30-9).</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>logging monitor level</strong> Limit messages logged to the terminal lines. By default, the terminal receives debugging messages and numerically lower levels (see Table 30-3 on page 30-9).</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>logging trap level</strong> Limit messages logged to the syslog servers. By default, syslog servers receive informational messages and numerically lower levels (see Table 30-3 on page 30-9). For complete syslog server configuration steps, see the “Configuring UNIX Syslog Servers” section on page 30-11.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>end</strong> Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>show running-config</strong> or <strong>show logging</strong> Verify your entries.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>copy running-config startup-config</strong> (Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

**Note**

Specifying a *level* causes messages at that level and numerically lower levels to be displayed at the destination.

To disable logging to the console, use the **no logging console** global configuration command. To disable logging to a terminal other than the console, use the **no logging monitor** global configuration command. To disable logging to syslog servers, use the **no logging trap** global configuration command.
Table 30-3 describes the level keywords. It also lists the corresponding UNIX syslog definitions from the most severe level to the least severe level.

<table>
<thead>
<tr>
<th>Level Keyword</th>
<th>Level</th>
<th>Description</th>
<th>Syslog Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>emergencies</td>
<td>0</td>
<td>System unstable</td>
<td>LOG_EMERG</td>
</tr>
<tr>
<td>alerts</td>
<td>1</td>
<td>Immediate action needed</td>
<td>LOG_ALERT</td>
</tr>
<tr>
<td>critical</td>
<td>2</td>
<td>Critical conditions</td>
<td>LOG_CRIT</td>
</tr>
<tr>
<td>errors</td>
<td>3</td>
<td>Error conditions</td>
<td>LOG_ERR</td>
</tr>
<tr>
<td>warnings</td>
<td>4</td>
<td>Warning conditions</td>
<td>LOG_WARNING</td>
</tr>
<tr>
<td>notifications</td>
<td>5</td>
<td>Normal but significant condition</td>
<td>LOG_NOTICE</td>
</tr>
<tr>
<td>informational</td>
<td>6</td>
<td>Informational messages only</td>
<td>LOG_INFO</td>
</tr>
<tr>
<td>debugging</td>
<td>7</td>
<td>Debugging messages</td>
<td>LOG_DEBUG</td>
</tr>
</tbody>
</table>

The software generates four other categories of messages:

- Error messages about software or hardware malfunctions, displayed at levels warnings through emergencies. These types of messages mean that the functionality of the switch is affected. For information on how to recover from these malfunctions, see the system message guide for this release.

- Output from the debug commands, displayed at the debugging level. Debug commands are typically used only by the Technical Assistance Center.

- Interface up or down transitions and system restart messages, displayed at the notifications level. This message is only for information; switch functionality is not affected.

- Reload requests and low-process stack messages, displayed at the informational level. This message is only for information; switch functionality is not affected.

**Limiting Syslog Messages Sent to the History Table and to SNMP**

If you enabled syslog message traps to be sent to an SNMP network management station by using the snmp-server enable trap global configuration command, you can change the level of messages sent and stored in the switch history table. You also can change the number of messages that are stored in the history table.

Messages are stored in the history table because SNMP traps are not guaranteed to reach their destination. By default, one message of the level warning and numerically lower levels (see Table 30-3 on page 30-9) are stored in the history table even if syslog traps are not enabled.
Beginning in privileged EXEC mode, follow these steps to change the level and history table size defaults. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Enter global configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>logging history level¹</td>
</tr>
<tr>
<td>Change the default level of syslog messages stored in the history file and sent to the SNMP server.</td>
<td></td>
</tr>
<tr>
<td>See Table 30-3 on page 30-9 for a list of level keywords.</td>
<td></td>
</tr>
<tr>
<td>By default, warnings, errors, critical, alerts, and emergencies messages are sent.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>logging history size number</td>
</tr>
<tr>
<td>Specify the number of syslog messages that can be stored in the history table.</td>
<td></td>
</tr>
<tr>
<td>The default is to store one message. The range is 0 to 500 messages.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>end</td>
</tr>
<tr>
<td>Return to privileged EXEC mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>show running-config</td>
</tr>
<tr>
<td>Verify your entries.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>copy running-config startup-config</td>
</tr>
<tr>
<td>(Optional) Save your entries in the configuration file.</td>
<td></td>
</tr>
</tbody>
</table>

When the history table is full (it contains the maximum number of message entries specified with the logging history size global configuration command), the oldest message entry is deleted from the table to allow the new message entry to be stored.

To return the logging of syslog messages to the default level, use the no logging history global configuration command. To return the number of messages in the history table to the default value, use the no logging history size global configuration command.

### Enabling the Configuration-Change Logger

You can enable a configuration logger to keep track of configuration changes made with the command-line interface (CLI). When you enter the logging enable configuration-change logger configuration command, the log records the session, the user, and the command that was entered to change the configuration. You can configure the size of the configuration log from 1 to 1000 entries (the default is 100). You can clear the log at any time by entering the no logging enable command followed by the logging enable command to disable and re-enable logging.

Use the show archive log config {all | number [end-number] | user username [session number] number [end-number] | statistics} [provisioning] privileged EXEC command to display the complete configuration log or the log for specified parameters.

The default is that configuration logging is disabled.

For information about the commands, see the Cisco IOS Configuration Fundamentals and Network Management Command Reference, Release 12.3 T at this URL:

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 archive</td>
<td>Enter archive configuration mode.</td>
</tr>
<tr>
<td>Step 3 log config</td>
<td>Enter configuration-change logger configuration mode.</td>
</tr>
<tr>
<td>Step 4 logging enable</td>
<td>Enable configuration change logging.</td>
</tr>
<tr>
<td>Step 5 logging size entries</td>
<td>(Optional) Configure the number of entries retained in the configuration log. The range is from 1 to 1000. The default is 100. Note: When the configuration log is full, the oldest log entry is removed each time a new entry is entered.</td>
</tr>
<tr>
<td>Step 6 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 7 show archive log config</td>
<td>Verify your entries by viewing the configuration log.</td>
</tr>
</tbody>
</table>

This example shows how to enable the configuration-change logger and to set the number of entries in the log to 500.

```
Switch(config)# archive
Switch(config-archive)# log config
Switch(config-archive-log-cfg)# logging enable
Switch(config-archive-log-cfg)# logging size 500
Switch(config-archive-log-cfg)# end
```

This is an example of output for the configuration log:

```
Switch# show archive log config all
idx sess user@line                      Logged command
 38  11 unknown user@vty3               |no aaa authorization config-commands
 39  12 unknown user@vty3               |no aaa authorization network default group radius
 40  12 unknown user@vty3               |no aaa accounting dot1x default start-stop group
 41  13 unknown user@vty3               |no aaa accounting system default
 42  14 temi@vty4                       |interface GigabitEthernet4/0/1
 43  14 temi@vty4                       |switchport mode trunk
 44  14 temi@vty4                       |exit
 45  16 temi@vty5                       |interface FastEthernet5/0/1
 46  16 temi@vty5                       |switchport mode trunk
 47  16 temi@vty5                       |exit
```

**Configuring UNIX Syslog Servers**

The next sections describe how to configure the UNIX server syslog daemon and how to define the UNIX system logging facility.

**Logging Messages to a UNIX Syslog Daemon**

Before you can send system log messages to a UNIX syslog server, you must configure the syslog daemon on a UNIX server. This procedure is optional.
Log in as root, and perform these steps:

**Note**
Some recent versions of UNIX syslog daemons no longer accept by default syslog packets from the network. If this is the case with your system, use the UNIX `man syslogd` command to decide what options must be added to or removed from the syslog command line to enable logging of remote syslog messages.

**Step 1**
Add a line such as the following to the file `/etc/syslog.conf`:

```
local7.debug /usr/adm/logs/cisco.log
```

The `local7` keyword specifies the logging facility to be used; see Table 30-4 on page 30-13 for information on the facilities. The `debug` keyword specifies the syslog level; see Table 30-3 on page 30-9 for information on the severity levels. The syslog daemon sends messages at this level or at a more severe level to the file specified in the next field. The file must already exist, and the syslog daemon must have permission to write to it.

**Step 2**
Create the log file by entering these commands at the UNIX shell prompt:

```
$ touch /var/log/cisco.log
$ chmod 666 /var/log/cisco.log
```

**Step 3**
Make sure the syslog daemon reads the new changes:

```
$ kill -HUP `cat /etc/syslog.pid`
```

For more information, see the `man syslog.conf` and `man syslogd` commands on your UNIX system.

**Configuring the UNIX System Logging Facility**

When sending system log messages to an external device, you can cause the switch to identify its messages as originating from any of the UNIX syslog facilities.

Beginning in privileged EXEC mode, follow these steps to configure UNIX system facility message logging. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>logging host</code></td>
</tr>
<tr>
<td></td>
<td>Log messages to a UNIX syslog server host by entering its IP address.</td>
</tr>
<tr>
<td></td>
<td>To build a list of syslog servers that receive logging messages, enter</td>
</tr>
<tr>
<td></td>
<td>this command more than once.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>logging trap level</code></td>
</tr>
<tr>
<td></td>
<td>Limit messages logged to the syslog servers.</td>
</tr>
<tr>
<td></td>
<td>Be default, syslog servers receive informational messages and lower.</td>
</tr>
<tr>
<td></td>
<td>See Table 30-3 on page 30-9 for <code>level</code> keywords.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>logging facility facility-type</code></td>
</tr>
<tr>
<td></td>
<td>Configure the syslog facility. See Table 30-4 on page 30-13 for</td>
</tr>
<tr>
<td></td>
<td><code>facility-type</code> keywords.</td>
</tr>
<tr>
<td></td>
<td>The default is <code>local7</code>.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>end</code></td>
</tr>
<tr>
<td></td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
To remove a syslog server, use the `no logging host` global configuration command, and specify the syslog server IP address. To disable logging to syslog servers, enter the `no logging trap` global configuration command.

Table 30-4 lists the UNIX system facilities supported by the software. For more information about these facilities, consult the operator’s manual for your UNIX operating system.

<table>
<thead>
<tr>
<th>Facility Type Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth</td>
<td>Authorization system</td>
</tr>
<tr>
<td>cron</td>
<td>Cron facility</td>
</tr>
<tr>
<td>daemon</td>
<td>System daemon</td>
</tr>
<tr>
<td>kern</td>
<td>Kernel</td>
</tr>
<tr>
<td>local0-7</td>
<td>Locally defined messages</td>
</tr>
<tr>
<td>lpr</td>
<td>Line printer system</td>
</tr>
<tr>
<td>mail</td>
<td>Mail system</td>
</tr>
<tr>
<td>news</td>
<td>USENET news</td>
</tr>
<tr>
<td>sys9-14</td>
<td>System use</td>
</tr>
<tr>
<td>syslog</td>
<td>System log</td>
</tr>
<tr>
<td>user</td>
<td>User process</td>
</tr>
<tr>
<td>uucp</td>
<td>UNIX-to-UNIX copy system</td>
</tr>
</tbody>
</table>

### Displaying the Logging Configuration

To display the logging configuration and the contents of the log buffer, use the `show logging` privileged EXEC command. For information about the fields in this display, see the *Cisco IOS Configuration Fundamentals Command Reference, Release 12.2.*
CHAPTER 31

Configuring SNMP

This chapter describes how to configure the Simple Network Management Protocol (SNMP) on the Catalyst 3750 Metro switch.

**Note**

For complete syntax and usage information for the commands used in this chapter, see the command reference for this release and the *Cisco IOS Network Management Command Reference, Release 12.4* from the Cisco.com page at this URL: http://www.cisco.com/en/US/docs/ios/netmgmt/command/reference/nm_book.html

For commands for MIB bulk statistics data collection and process MIB configuration, see the *Cisco IOS Commands Master List, Release 12.4*, at this URL: http://www.cisco.com/en/US/products/ps6350/products_product_indices_list.html

This chapter consists of these sections:

- Understanding SNMP, page 31-1
- Configuring SNMP, page 31-7
- Displaying SNMP Status, page 31-24

**Understanding SNMP**

SNMP is an application-layer protocol that provides a message format for communication between managers and agents. The SNMP system consists of an SNMP manager, an SNMP agent, and a MIB. The SNMP manager can be part of a network management system (NMS) such as CiscoWorks. The agent and MIB reside on the switch. To configure SNMP on the switch, you define the relationship between the manager and the agent.

The SNMP agent contains MIB variables whose values the SNMP manager can request or change. A manager can get a value from an agent or store a value into the agent. The agent gathers data from the MIB, the repository for information about device parameters and network data. The agent can also respond to a manager’s requests to get or set data.

An agent can send unsolicited traps to the manager. Traps are messages alerting the SNMP manager to a condition on the network. Traps can mean improper user authentication, restarts, link status (up or down), MAC address tracking, closing of a Transmission Control Protocol (TCP) connection, loss of connection to a neighbor, or other significant events.
Although the switch does not support the Cisco Data Collection MIB, starting with Cisco IOS Release 12.2(37)SE, you can use the command-line interface to periodically transfer selected MIB data to specified NMS stations. Starting with this release, you can also configure a Cisco Process MIB CPU threshold table.

This section includes information about these topics:
- SNMP Versions, page 31-2
- SNMP Manager Functions, page 31-4
- SNMP Agent Functions, page 31-4
- SNMP Community Strings, page 31-4
- Using SNMP to Access MIB Variables, page 31-5
- SNMP Notifications, page 31-5
- SNMP ifIndex MIB Object Values, page 31-6
- MIB Data Collection and Transfer, page 31-6

### SNMP Versions

This software release supports these SNMP versions:

- **SNMPv1**—The Simple Network Management Protocol, a Full Internet Standard, defined in RFC 1157.
- **SNMPv2**—Version 2 of the Simple Network Management Protocol, a Draft Internet Standard, defined in RFCs 1902 through 1907.
- **SNMPv2C**—The community-string-based Administrative Framework for SNMPv2, an Experimental Internet Protocol defined in RFC 1901.
- **SNMPv3**—Version 3 of the SNMP is an interoperable standards-based protocol defined in RFCs 2273 to 2275. SNMPv3 provides secure access to devices by authenticating and encrypting packets over the network and includes these security features:
  - Message integrity—ensuring that a packet was not tampered with in transit
  - Authentication—determining that the message is from a valid source
  - Encryption—mixing the contents of a package to prevent it from being read by an unauthorized source.

**Note**  To select encryption, enter the `priv` keyword. This keyword is available only when the crypto (encrypted) software image is installed.

Both SNMPv1 and SNMPv2C use a community-based form of security. The community of managers able to access the agent’s MIB is defined by an IP address access control list and password.
SNMPv2C includes a bulk retrieval mechanism and more detailed error message reporting to management stations. The bulk retrieval mechanism retrieves tables and large quantities of information, minimizing the number of round-trips required. The SNMPv2C improved error-handling includes expanded error codes that distinguish different kinds of error conditions; these conditions are reported through a single error code in SNMPv1. Error return codes in SNMPv2C report the error type.

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy set up for a user and the group within which the user resides. A security level is the permitted level of security within a security model. A combination of the security level and the security model determine which security mechanism is used when handling an SNMP packet. Available security models are SNMPv1, SNMPv2C, and SNMPv3.

Table 31-1 identifies the characteristics of the different combinations of security models and levels.

<table>
<thead>
<tr>
<th>Model</th>
<th>Level</th>
<th>Authentication</th>
<th>Encryption</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMPv1</td>
<td>noAuthNoPriv</td>
<td>Community string</td>
<td>No</td>
<td>Uses a community string match for authentication.</td>
</tr>
<tr>
<td>SNMPv2C</td>
<td>noAuthNoPriv</td>
<td>Community string</td>
<td>No</td>
<td>Uses a community string match for authentication.</td>
</tr>
<tr>
<td>SNMPv3</td>
<td>noAuthNoPriv</td>
<td>Username</td>
<td>No</td>
<td>Uses a username match for authentication.</td>
</tr>
<tr>
<td>SNMPv3</td>
<td>authNoPriv</td>
<td>Message Digest 5 (MD5)</td>
<td>No</td>
<td>Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.</td>
</tr>
<tr>
<td></td>
<td>(requires the cryptographic software image)</td>
<td>or Secure Hash Algorithm (SHA)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SNMPv3</td>
<td>authPriv</td>
<td>MD5 or SHA</td>
<td>Data Encryption Standard (DES) or Advanced Encryption Standard (AES)</td>
<td>Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Allows specifying the User-based Security Model (USM) with these encryption algorithms:</td>
</tr>
<tr>
<td></td>
<td>(requires the cryptographic software image)</td>
<td></td>
<td></td>
<td>- DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- 3DES 168-bit encryption</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- AES 128-bit, 192-bit, or 256-bit encryption</td>
</tr>
</tbody>
</table>

You must configure the SNMP agent to use the SNMP version supported by the management station. Because an agent can communicate with multiple managers, you can configure the software to support communications using SNMPv1, and SNMPv2C, and SNMPv3 protocols.
SNMP Manager Functions

The SNMP manager uses information in the MIB to perform the operations described in Table 31-2.

Table 31-2  SNMP Operations

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>get-request</td>
<td>Retrieves a value from a specific variable.</td>
</tr>
<tr>
<td>get-next-request</td>
<td>Retrieves a value from a variable within a table.</td>
</tr>
<tr>
<td>get-bulk-request</td>
<td>Retrieves large blocks of data, such as multiple rows in a table, that would otherwise require the transmission of many small blocks of data.</td>
</tr>
<tr>
<td>get-response</td>
<td>Replies to a get-request, get-next-request, and set-request sent by an NMS.</td>
</tr>
<tr>
<td>set-request</td>
<td>Stores a value in a specific variable.</td>
</tr>
<tr>
<td>trap</td>
<td>An unsolicited message sent by an SNMP agent to an SNMP manager when some event has occurred.</td>
</tr>
</tbody>
</table>

1. With this operation, an SNMP manager does not need to know the exact variable name. A sequential search is performed to find the needed variable from within a table.
2. The get-bulk command only works with SNMPv2 or later.

SNMP Agent Functions

The SNMP agent responds to SNMP manager requests as follows:

- Get a MIB variable—The SNMP agent begins this function in response to a request from the NMS. The agent retrieves the value of the requested MIB variable and responds to the NMS with that value.
- Set a MIB variable—The SNMP agent begins this function in response to a message from the NMS. The SNMP agent changes the value of the MIB variable to the value requested by the NMS.

The SNMP agent also sends unsolicited trap messages to notify an NMS that a significant event has occurred on the agent. Examples of trap conditions include, but are not limited to, when a port or module goes up or down, when spanning-tree topology changes occur, and when authentication failures occur.

SNMP Community Strings

SNMP community strings authenticate access to MIB objects and function as embedded passwords. In order for the NMS to access the switch, the community string definitions on the NMS must match at least one of the three community string definitions on the switch.

A community string can have one of these attributes:

- Read-only (RO)—Gives read access to authorized management stations to all objects in the MIB except the community strings, but does not allow write access
- Read-write (RW)—Gives read and write access to authorized management stations to all objects in the MIB, but does not allow access to the community strings
- Read-write-all—Gives read and write access to authorized management stations to all objects in the MIB, including the community strings
Using SNMP to Access MIB Variables

An example of an NMS is the CiscoWorks network management software. CiscoWorks 2000 software uses the 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 to troubleshoot internetworking problems, increase network performance, verify the configuration of devices, monitor traffic loads, and more.

As shown in Figure 31-1, the SNMP agent gathers data from the MIB. The agent can send traps, or notification of certain events, to the SNMP manager, which receives and processes the traps. Traps alert the SNMP manager to a condition on the network such as improper user authentication, restarts, link status (up or down), MAC address tracking, and so forth. The SNMP agent also responds to MIB-related queries sent by the SNMP manager in `get-request`, `get-next-request`, and `set-request` format.

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

SNMP Notifications

SNMP allows the switch to send notifications to SNMP managers when particular events occur. SNMP notifications can be sent as traps or inform requests. In command syntax, unless there is an option in the command to select either traps or informs, the keyword ` traps` refers to either traps or informs, or both. Use the `snmp-server host` command to specify whether to send SNMP notifications as traps or informs.

Note

SNMPv1 does not support informs.

Traps are unreliable because the receiver does not send an acknowledgment when it receives a trap, and the sender cannot determine if the trap was received. When an SNMP manager receives an inform request, it acknowledges the message with an SNMP response protocol data unit (PDU). If the sender does not receive a response, the inform request can be sent again. Because they can be re-sent, informs are more likely than traps to reach their intended destination.

The characteristics that make informs more reliable than traps also consume more resources in the switch and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request is held in memory until a response is received or the request times out. Traps are sent only once, but an inform might be re-sent or retried several times. The retries increase traffic and contribute to a higher overhead on the network. Therefore, traps and informs require a trade-off between reliability and resources. If it is important that the SNMP manager receive every notification, use inform requests. If traffic on the network or memory in the switch is a concern and notification is not required, use traps.
SNMP \textit{ifIndex} MIB Object Values

In an NMS, the IF-MIB generates and assigns an interface index (\textit{ifIndex}) object value that is a unique number greater than zero to identify a physical or a logical interface. When the switch reboots or the switch software is upgraded, the switch uses this same value for the interface. For example, if the switch assigns a port 2 an \textit{ifIndex} value of 10003, this value is the same after the switch reboots.

The switch uses one of the values in Table 31-3 to assign an \textit{ifIndex} value to an interface:

\begin{table}[h]
\centering
\begin{tabular}{|l|l|}
\hline
\textbf{Interface Type} & \textbf{\textit{ifIndex} Range} \\
\hline
SVI\textsuperscript{1} & 1–4999 \\
EtherChannel & 5000–5012 \\
Loopback & 5013–5077 \\
Tunnel & 5078–5142 \\
Physical (such as Gigabit Ethernet or SFP\textsuperscript{2}-module interfaces) & 10000–14500 \\
Null & 14501 \\
\hline
\end{tabular}
\caption{\textit{ifIndex} Values}
\end{table}

1. SVI = switch virtual interface
2. SFP = small form-factor pluggable

\begin{itemize}
\item The switch might not use sequential values within a range.
\end{itemize}

MIB Data Collection and Transfer

To configure periodic transfer MIB data from a device to a specified NMS, you group data from multiple MIBs into list and configure a polling interval. All MIB objects in the list are polled at the specified interval, and the data is transferred to the specified NMS at a configured transfer interval. The periodic data collection and transfer mechanism is referred to as the \textit{bulk-statistics} feature.

To configure bulk statistics, you use a bulk-statistics object list to specify the SNMP object types to be monitored and a bulk-statistics schema to specify the instances of the objects to be collected. You can specify MIBs, MIB tables, MIB objects, and object indices by using a series of object identifiers (OIDs).

- A bulk-statistics object list is a user-specified set of MIB objects that share the same MIB index identified by a user-specified name.
- A bulk-statistics schema is identified by a user-specified name and includes the name of the object list, the instance to be retrieved for objects in the object list, and the polling interval.

After you configure the data to be collected, a single virtual bulk-statistics file is created with all the collected data. You can specify how the file is transferred to the NMS (FTP, RCP, or TFTP), how often the file is transferred (the default is 30 minutes), and a secondary destination if the primary NMS is not available. The transfer-interval time is also the collection-interval time. After the collection interval ends, the bulk-statistics file is frozen, and a new local bulk-statistics file is created to store new data. The frozen file is transferred to the specified destination and then deleted (unless you configure the device to keep the file in memory for a specified time period). You can configure the switch to send an SNMP notification to the NMS if a transfer is not successful and to enter a syslog message on the local device.
Configuring SNMP

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

- Default SNMP Configuration, page 31-7
- SNMP Configuration Guidelines, page 31-7
- Disabling the SNMP Agent, page 31-8
- Configuring Community Strings, page 31-8
- Configuring SNMP Groups and Users, page 31-10
- Configuring SNMP Notifications, page 31-12
- Setting the Agent Contact and Location Information, page 31-17
- Limiting TFTP Servers Used Through SNMP, page 31-18
- Configuring MIB Data Collection and Transfer, page 31-19
- Configuring the Cisco Process MIB CPU Threshold Table, page 31-22
- SNMP Examples, page 31-23

Default SNMP Configuration

Table 31-4 shows the default SNMP configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP agent</td>
<td>Disabled(^1).</td>
</tr>
<tr>
<td>SNMP trap receiver</td>
<td>None configured</td>
</tr>
<tr>
<td>SNMP traps</td>
<td>None enabled except the trap for TCP connections (tty)</td>
</tr>
<tr>
<td>SNMP version</td>
<td>If no version keyword is present, the default is Version 1.</td>
</tr>
<tr>
<td>SNMPv3 authentication</td>
<td>If no keyword is entered, the default is the noauth (noAuthNoPriv) security level.</td>
</tr>
<tr>
<td>SNMP notification type</td>
<td>If no type is specified, all notifications are sent.</td>
</tr>
</tbody>
</table>

1. This is the default at switch startup when the startup configuration does not have any snmp-server global configuration commands.

SNMP Configuration Guidelines

An SNMP group is a table that maps SNMP users to SNMP views. An SNMP user is a member of an SNMP group. An SNMP host is the recipient of an SNMP trap operation. An SNMP engine ID is a name for the local or remote SNMP engine.

When configuring SNMP, follow these guidelines:

- When configuring an SNMP group, do not specify a notify view. The snmp-server host global configuration command autogenerates a notify view for the user and then adds it to the group associated with that user. Modifying the group's notify view affects all users associated with that group. For information about when you should configure notify views, see the Cisco IOS Configuration Fundamentals Command Reference, Release 12.2.
To configure a remote user, specify the IP address or port number for the remote SNMP agent of the device where the user resides.

Before you configure remote users for a particular agent, configure the SNMP engine ID, using the `snmp-server engineID` global configuration with the `remote` option. The remote agent's SNMP engine ID and user password are used to compute the authentication and privacy digests. If you do not configure the remote engine ID first, the configuration command fails.

When configuring SNMP informs, you need to configure the SNMP engine ID for the remote agent in the SNMP database before you can send proxy requests or informs to it.

If a local user is not associated with a remote host, the switch does not send informs for the `auth` (authNoPriv) and the `priv` (authPriv) authentication levels.

Changing the value of the SNMP engine ID has important side effects. A user's password (entered on the command line) is converted to an MD5 or SHA security digest based on the password and the local engine ID. The command-line password is then destroyed, as required by RFC 2274. Because of this deletion, if the value of the engine ID changes, the security digests of SNMPv3 users become invalid, and you need to reconfigure SNMP users by using the `snmp-server user` global configuration command. Similar restrictions require the reconfiguration of community strings when the engine ID changes.

### Disabling the SNMP Agent

Beginning in privileged EXEC mode, follow these steps to disable the SNMP agent:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>no snmp-server</code></td>
<td>Disable the SNMP agent operation.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td><code>show running-config</code></td>
<td>Verify your entries.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

The `no snmp-server` global configuration command disables all running versions (Version 1, Version 2C, and Version 3) on the device. No specific IOS command exists to enable SNMP. The first `snmp-server` global configuration command that you enter enables all versions of SNMP.

### Configuring Community Strings

You use the SNMP community string to define the relationship between the SNMP manager and the agent. The community string acts like a password to permit access to the agent on the switch. Optionally, you can specify one or more of these characteristics associated with the string:

- An access list of IP addresses of the SNMP managers that are permitted to use the community string to gain access to the agent
- A MIB view, which defines the subset of all MIB objects accessible to the given community
- Read and write or read-only permission for the MIB objects accessible to the community
Beginning in privileged EXEC mode, follow these steps to configure a community string on the switch:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
</tbody>
</table>
| **Step 2** | snmp-server community string [view view-name] [ro | rw] [access-list-number] | Configure the community string.  
| | | Note The @ symbol is used for delimiting the context information. Avoid using the @ symbol as part of the SNMP community string when configuring this command. |
| | | • For *string*, specify a string that acts like a password and permits access to the SNMP protocol. You can configure one or more community strings of any length. |
| | | • (Optional) For *view*, specify the view record accessible to the community. |
| | | • (Optional) Specify either read-only (*ro*) if you want authorized management stations to retrieve MIB objects, or specify read-write (*rw*) if you want authorized management stations to retrieve and modify MIB objects. By default, the community string permits read-only access to all objects. |
| | | • (Optional) For *access-list-number*, enter an IP standard access list numbered from 1 to 99 and 1300 to 1999. |
| **Step 3** | access-list access-list-number {deny | permit} source [source-wildcard] | (Optional) If you specified an IP standard access list number in Step 2, then create the list, repeating the command as many times as necessary. |
| | | • For *access-list-number*, enter the access list number specified in Step 2. |
| | | • The deny keyword denies access if the conditions are matched. The permit keyword permits access if the conditions are matched. |
| | | • For *source*, enter the IP address of the SNMP managers that are permitted to use the community string to gain access to the agent. |
| | | • (Optional) For *source-wildcard*, enter the wildcard bits in dotted decimal notation to be applied to the source. Place ones in the bit positions that you want to ignore. |
| | | Recall that the access list is always terminated by an implicit deny statement for everything. |
| **Step 4** | end | Return to privileged EXEC mode. |
| **Step 5** | show running-config | Verify your entries. |
| **Step 6** | copy running-config startup-config | (Optional) Save your entries in the configuration file. |

**Note** To disable access for an SNMP community, set the community string for that community to the null string (do not enter a value for the community string).
To remove a specific community string, use the `no snmp-server community string` global configuration command.

This example shows how to assign the string `comaccess` to SNMP, to allow read-only access, and to specify that IP access list 4 can use the community string to gain access to the switch SNMP agent:

```
Switch(config)# snmp-server community comaccess ro 4
```

### Configuring SNMP Groups and Users

You can specify an identification name (engine ID) for the local or remote SNMP server engine on the switch. You can configure an SNMP server group that maps SNMP users to SNMP views, and you can add new users to the SNMP group.

Beginning in privileged EXEC mode, follow these steps to configure SNMP on the switch:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2: snmp-server engineID {local engineid-string</td>
<td>remote ip-address [udp-port port-number] engineid-string}</td>
</tr>
<tr>
<td></td>
<td>• The <code>engineid-string</code> is a 24-character ID string with the name of the copy of SNMP. You need not specify the entire 24-character engine ID if it has trailing zeros. Specify only the portion of the engine ID up to the point where only zeros remain in the value. For example, to configure an engine ID of 123400000000000000000000, you can enter this: <code>snmp-server engineID local 1234</code></td>
</tr>
<tr>
<td></td>
<td>• If you select <code>remote</code>, specify the <code>ip-address</code> of the device that contains the remote copy of SNMP and the optional UDP port on the remote device. The default is 162.</td>
</tr>
</tbody>
</table>
Chapter 31 Configuring SNMP

Step 3

```
snmp-server group groupname {v1 | v2c | v3 [auth | noauth | priv]} [read readview] [write writeview] [notify notifyview] [access access-list]
```

Configure a new SNMP group on the remote device.

- For `groupname`, specify the name of the group.
- Specify a security model:
  - `v1` is the least secure of the possible security models.
  - `v2c` is the second least secure model. It allows transmission of informs and integers twice the normal width.
  - `v3`, the most secure, requires you to select an authentication level:
    - `auth`—Enables the Message Digest 5 (MD5) and the Secure Hash Algorithm (SHA) packet authentication.
    - `noauth`—The noAuthNoPriv security level. This is the default if no keyword is specified.
    - `priv`—Enables Data Encryption Standard (DES) packet encryption (also called `privacy`).

**Note** The `priv` keyword is available only when the crypto software image is installed.

- (Optional) Enter `read readview` with a string (not to exceed 64 characters) that is the name of the view in which you can only view the contents of the agent.
- (Optional) Enter `write writeview` with a string (not to exceed 64 characters) that is the name of the view in which you enter data and configure the contents of the agent.
- (Optional) Enter `notify notifyview` with a string (not to exceed 64 characters) that is the name of the view in which you specify a notify, inform, or trap.
- (Optional) Enter `access access-list` with a string (not to exceed 64 characters) that is the name of the access list.
### Configuring SNMP Notifications

A trap manager is a management station that receives and processes traps. Traps are system alerts that the switch generates when certain events occur. By default, no trap manager is defined, and no traps are sent. Switches running this IOS release can have an unlimited number of trap managers.

#### Step 4

```plaintext
snmp-server user username groupname
[remote host [udp-port port]] {v1 [access access-list] | v2c [access access-list] | v3 [encrypted] [access access-list] [auth {md5 | sha} auth-password] | [priv {des | 3des | aes {128 | 192 | 256}} priv-password]
```

Add a new user for an SNMP group.

- The **username** is the name of the user on the host that connects to the agent.
- The **groupname** is the name of the group to which the user is associated.

- Enter **remote** to specify a remote SNMP entity to which the user belongs and the hostname or IP address of that entity with the optional UDP port number. The default is 162.

- Enter the SNMP version number (**v1, v2c, or v3**). If you enter **v3**, you have these additional options:
  - **encrypted** specifies that the password appears in encrypted format. This keyword is available only when the **v3** keyword is specified.
  - **auth** is an authentication level setting session that can be either the HMAC-MD5-96 (**md5**) or the HMAC-SHA-96 (**sha**) authentication level and requires a password string **auth-password** (not to exceed 64 characters).

- If you enter **v3** and the switch is running the cryptographic software image, you can also configure a private (**priv**) encryption algorithm and password string **priv-password** (not to exceed 64 characters).
  - **priv** specifies the User-based Security Model (USM).
  - **des** specifies the use of the 56-bit DES algorithm.
  - **3des** specifies the use of the 168-bit DES algorithm.
  - **aes** specifies the use of the DES algorithm. You must select either 128-bit, 192-bit, or 256-bit encryption.

- (Optional) Enter **access access-list** with a string (not to exceed 64 characters) that is the name of the access list.

#### Step 5

```plaintext
end
```

Return to privileged EXEC mode.

#### Step 6

```plaintext
show running-config
```

Verify your entries.

**Note** To display SNMPv3 information about **auth | noauth | priv** mode configuration, you must enter the **show snmp user** privileged command.

#### Step 7

```plaintext
copy running-config startup-config
```

(Optional) Save your entries in the configuration file.
**Note**

Many commands use the word *traps* in the command syntax. Unless there is an option in the command to select either traps or informs, the keyword *traps* refers to traps, informs, or both. Use the `snmp-server host` command to specify whether to send SNMP notifications as traps or informs.
Table 31-5 describes some of the supported switch traps (notification types). You can enable any or all of these traps and configure a trap manager to receive them.

**Note**
Although visible in the command-line interface (CLI) online help, the `fru-ctrl` keyword is not supported.

### Table 31-5 Switch Notification Types

<table>
<thead>
<tr>
<th>Notification Type Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgp</td>
<td>Generates BGP state change traps. This option is only available when the enhanced multilayer image is installed.</td>
</tr>
<tr>
<td>bridge</td>
<td>Generates STP bridge MIB traps.</td>
</tr>
<tr>
<td>bulkstat collection transfer</td>
<td>Generates a trap when an unsuccessful data collection or data transfer occurs or when the bulkstats file reaches the maximum size.</td>
</tr>
<tr>
<td>cluster</td>
<td>Generates a trap when the cluster configuration changes.</td>
</tr>
<tr>
<td>config</td>
<td>Generates a trap for SNMP configuration changes.</td>
</tr>
<tr>
<td>copy-config</td>
<td>Generates a trap for SNMP copy configuration changes.</td>
</tr>
<tr>
<td>cpu threshold</td>
<td>Generates a trap for CPU threshold violations</td>
</tr>
<tr>
<td>entity</td>
<td>Generates a trap for SNMP entity changes.</td>
</tr>
<tr>
<td>envmon</td>
<td>Generates environmental monitor traps. You can enable any or all of these environmental traps: fan, shutdown, supply, temperature.</td>
</tr>
<tr>
<td>flash</td>
<td>Generates SNMP FLASH notifications.</td>
</tr>
<tr>
<td>hsrp</td>
<td>Generates a trap for Hot Standby Router Protocol (HSRP) changes.</td>
</tr>
<tr>
<td>ipmulticast</td>
<td>Generates a trap for IP multicast routing changes.</td>
</tr>
<tr>
<td>mac-notification</td>
<td>Generates a trap for MAC address notifications.</td>
</tr>
<tr>
<td>msdp</td>
<td>Generates a trap for Multicast Source Discovery Protocol (MSDP) changes.</td>
</tr>
<tr>
<td>ospf</td>
<td>Generates a trap for Open Shortest Path First (OSPF) changes. You can enable any or all of these traps: Cisco specific, errors, link-state advertisement, rate limit, retransmit, and state changes.</td>
</tr>
<tr>
<td>pim</td>
<td>Generates a trap for Protocol-Independent Multicast (PIM) changes. You can enable any or all of these traps: invalid PIM messages, neighbor changes, and rendezvous point (RP)-mapping changes.</td>
</tr>
<tr>
<td>port-security</td>
<td>Generates SNMP port security traps. You can also set a maximum trap rate per second. The range is from 0 to 1000; the default is 0, which means that there is no rate limit. <strong>Note</strong> When you configure a trap by using the notification type <code>port-security</code>, configure the port security trap first, and then configure the port security trap rate:</td>
</tr>
<tr>
<td></td>
<td>- <code>snmp-server enable traps port-security</code></td>
</tr>
<tr>
<td></td>
<td>- <code>snmp-server enable traps port-security trap-rate rate</code></td>
</tr>
<tr>
<td>rtr</td>
<td>Generates a trap for the SNMP Response Time Reporter (RTR).</td>
</tr>
</tbody>
</table>
### Table 31-5  Switch Notification Types (continued)

<table>
<thead>
<tr>
<th>Notification Type Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>snmp</td>
<td>Generates a trap for SNMP-type notifications for authentication, cold start, warm start, link up or link down.</td>
</tr>
<tr>
<td>storm-control</td>
<td>Generates a trap for SNMP storm-control. You can also set a maximum trap rate per minute. The range is from 0 to 1000; the default is 0 (no limit is imposed; a trap is sent at every occurrence).</td>
</tr>
<tr>
<td>stpx</td>
<td>Generates SNMP STP Extended MIB traps.</td>
</tr>
<tr>
<td>syslog</td>
<td>Generates SNMP syslog traps.</td>
</tr>
<tr>
<td>tty</td>
<td>Generates a trap for TCP connections. This trap is enabled by default.</td>
</tr>
<tr>
<td>vlan-membership</td>
<td>Generates a trap for SNMP VLAN membership changes.</td>
</tr>
<tr>
<td>vlancreate</td>
<td>Generates SNMP VLAN created traps.</td>
</tr>
<tr>
<td>vlandelete</td>
<td>Generates SNMP VLAN deleted traps.</td>
</tr>
<tr>
<td>vtp</td>
<td>Generates a trap for VLAN Trunking Protocol (VTP) changes.</td>
</tr>
</tbody>
</table>

**Note**

Though visible in the command-line help string, the `fru-ctrl` and flash `insertion` and `removal` keywords are not supported. The `snmp-server enable informs` command is not supported. To enable the sending of SNMP inform notifications, use the `snmp-server enable traps` command combined with the `snmp-server host host-addr informs` command.

You can use the `snmp-server host` global configuration command to a specific host to receive the notification types listed in Table 31-5.

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>snmp-server engineID remote ip-address engineid-string</code></td>
<td>Specify the engine ID for the remote host.</td>
</tr>
<tr>
<td>Step 3</td>
<td>`snmp-server user username [groupname remote host [udp-port port] [v1</td>
<td>v2c</td>
</tr>
</tbody>
</table>

**Note**

You cannot configure a remote user for an address without first configuring the engine ID for the remote host. If you try to configure the user before configuring the remote engine ID, you receive an error message, and the command is not executed.
## Configuring SNMP

### Command

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4</td>
<td>`snmp-server host host-addr [traps</td>
<td>informs] [version {1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- For <code>host-addr</code>, specify the name or Internet address of the host (the targeted recipient).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- (Optional) Enter <code>traps</code> (the default) to send SNMP traps to the host.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- (Optional) Enter <code>informs</code> to send SNMP informs to the host.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- (Optional) Specify the SNMP <code>version</code> (1, 2c, or 3). SNMPv1 does not support informs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- (Optional) For Version 3, select authentication level <code>auth</code>, <code>noauth</code>, or <code>priv</code>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td>The <code>priv</code> keyword is available only when the crypto software image is installed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- For <code>community-string</code>, enter the password-like community string sent with the notification operation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> The @ symbol is used for delimiting the context information. Avoid using the @ symbol as part of the SNMP community string when configuring this command.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- (Optional) For <code>udp-port port</code>, enter the remote device UDP port.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- (Optional) For <code>notification-type</code>, use the keywords listed in Table 31-5 on page 31-14. If no type is specified, all notifications are sent.</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>snmp-server enable traps notification-types</code></td>
<td>Enable the switch to send traps or informs and specify the type of notifications to be sent. For a list of notification types, see Table 31-5 on page 31-14, or enter this: <code>snmp-server enable traps ?</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>To enable multiple types of traps, you must enter a separate <code>snmp-server enable traps</code> command for each trap type.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td>When you configure a trap by using the notification type <code>port-security</code>, configure the port security trap first, and then configure the port security trap rate:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <code>snmp-server enable traps port-security</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <code>snmp-server enable traps port-security trap-rate rate</code></td>
</tr>
<tr>
<td>Step 6</td>
<td><code>snmp-server trap-source interface-id</code></td>
<td>(Optional) Specify the source interface, which provides the IP address for the trap message. This command also sets the source IP address for informs.</td>
</tr>
<tr>
<td>Step 7</td>
<td><code>snmp-server queue-length length</code></td>
<td>(Optional) Establish the message queue length for each trap host. The range is 1 to 1000; the default is 10.</td>
</tr>
<tr>
<td>Step 8</td>
<td><code>snmp-server trap-timeout seconds</code></td>
<td>(Optional) Define how often to resend trap messages. The range is 1 to 1000; the default is 30 seconds.</td>
</tr>
<tr>
<td>Step 9</td>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
Chapter 31      Configuring SNMP

Configuring SNMP

The `snmp-server host` command specifies which hosts receive the notifications. The `snmp-server enable trap` command globally enables the mechanism for the specified notification (for traps and informs). To enable a host to receive an inform, you must configure an `snmp-server host informs` command for the host and globally enable informs by using the `snmp-server enable traps` command.

To remove the specified host from receiving traps, use the `no snmp-server host` global configuration command. The `no snmp-server host` command with no keywords disables traps, but not informs, to the host. To disable informs, use the `no snmp-server host informs` global configuration command. To disable a specific trap type, use the `no snmp-server enable traps notification-types` global configuration command.

Setting the Agent Contact and Location Information

Beginning in privileged EXEC mode, follow these steps to set the system contact and location of the SNMP agent so that these descriptions can be accessed through the configuration file:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 snmp-server contact text</td>
<td>Set the system contact string.</td>
</tr>
<tr>
<td></td>
<td>For example: snmp-server contact Dial System Operator at beeper 21555.</td>
</tr>
<tr>
<td>Step 3 snmp-server location text</td>
<td>Set the system location string.</td>
</tr>
<tr>
<td></td>
<td>For example: snmp-server location Building 3/Room 222</td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5 show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 6 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
Limiting TFTP Servers Used Through SNMP

Beginning in privileged EXEC mode, follow these steps to limit the TFTP servers used for saving and loading configuration files through SNMP to the servers specified in an access list:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>snmp-server tftp-server-list access-list-number</td>
</tr>
</tbody>
</table>
| **Step 3** | access-list access-list-number { deny | permit } source [source-wildcard] | Create a standard access list, repeating the command as many times as necessary.  
  * For *access-list-number*, enter the access list number specified in Step 2.  
  * The *deny* keyword denies access if the conditions are matched. The *permit* keyword permits access if the conditions are matched.  
  * For *source*, enter the IP address of the TFTP servers that can access the switch.  
  * (Optional) For *source-wildcard*, enter the wildcard bits, in dotted decimal notation, to be applied to the source. Place ones in the bit positions that you want to ignore.  
Recall that the access list is always terminated by an implicit deny statement for everything. |
| **Step 4** | end | Return to privileged EXEC mode. |
| **Step 5** | show running-config | Verify your entries. |
| **Step 6** | copy running-config startup-config | (Optional) Save your entries in the configuration file. |

Setting the CPU Threshold Notification Types and Values

Beginning in privileged EXEC mode, follow these steps to set the CPU threshold notification types and values:

- **Command**: snmp-server trap-source
- **Purpose**: Set the CPU threshold notification types and values.
### Configuring SNMP

#### Configuring MIB Data Collection and Transfer

This section includes basic configuration for MIB data collection. For more information, see the *Periodic MIB Data Collection and Transfer Mechanism* feature module at this URL:


Beginning in privileged EXEC mode, follow these steps to configure a bulk-statistics object list and schema options:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Set the CPU threshold notification types and values:</td>
</tr>
<tr>
<td>process cpu threshold type { total</td>
<td>process</td>
</tr>
<tr>
<td></td>
<td>• process—set the notification type to CPU process utilization.</td>
</tr>
<tr>
<td></td>
<td>• interrupt—set the notification type to CPU interrupt utilization.</td>
</tr>
<tr>
<td></td>
<td>• rising percentage—the percentage (1 to 100) of CPU resources that,</td>
</tr>
<tr>
<td></td>
<td>when exceeded for the configured interval, sends a CPU threshold</td>
</tr>
<tr>
<td></td>
<td>notification.</td>
</tr>
<tr>
<td></td>
<td>• interval seconds—the duration of the CPU threshold violation in</td>
</tr>
<tr>
<td></td>
<td>seconds (5 to 86400) that, when met, sends a CPU threshold</td>
</tr>
<tr>
<td></td>
<td>notification.</td>
</tr>
<tr>
<td></td>
<td>• falling fall-percentage—the percentage (1 to 100) of CPU</td>
</tr>
<tr>
<td></td>
<td>resources that, when usage falls below this level for the configured</td>
</tr>
<tr>
<td></td>
<td>interval, sends a CPU threshold notification.</td>
</tr>
<tr>
<td></td>
<td>This value must be equal to or less than the rising percentage value.</td>
</tr>
<tr>
<td></td>
<td>If not specified, the falling fall-percentage value is the same as the</td>
</tr>
<tr>
<td></td>
<td>rising percentage value.</td>
</tr>
<tr>
<td><strong>Step 3</strong> end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong> show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td><strong>Step 5</strong> copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
## Configuring SNMP

**This example configures a bulk-statistics object list and schema:**

```plaintext
Switch(config)# snmp mib bulkstat object-list ifMIB
Switch(config-bulk-objects)# add 1.3.6.1.2.1.2.1.2.2.2.1.11
Switch(config-bulk-objects)# add ifName
Switch(config-bulk-objects)# exit
Switch(config)# snmp mib bulkstat schema testschema
Switch(config-bulk-sc)# object-list ifMIB
Switch(config-bulk-sc)# instance wild oil 1
Switch(config-bulk-sc)# poll-interval 1
Switch(config-bulk-sc)# exit
```

### Command Purpose

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td>`add {object-name</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>exit</code></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>snmp-server mib bulkstat schema schema-name</code></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>object-list list-name</code></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>`instance {exact</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><code>poll interval interval</code></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td><code>end</code></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td><code>copy running-config startup-config</code></td>
</tr>
</tbody>
</table>
Beginning in privileged EXEC mode, follow these steps to configure bulk-statistics transfer options:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>snmp-server mib bulkstat transfer transfer-id</td>
<td>Identify the transfer configuration with a name, and enter bulk-statistics transfer configuration mode.</td>
</tr>
<tr>
<td>3</td>
<td>buffer-size bytes</td>
<td>(Optional) Specify the maximum size for the bulk-statistics data file in bytes. The range is from 1024 to 2147483647 bytes; the default is 2048 bytes.</td>
</tr>
<tr>
<td>4</td>
<td>format {bulkBinary</td>
<td>bulkASCII</td>
</tr>
<tr>
<td>5</td>
<td>schema schema-name</td>
<td>Specify the bulk-statistics schema to be transferred. Repeat this command for as many schemas as desired. You can associate multiple schemas with a transfer configuration.</td>
</tr>
<tr>
<td>6</td>
<td>transfer-interval minutes</td>
<td>(Optional) Specify the length of time that the system should collect MIB data before attempting the transfer operation. The valid range is from 1 to 2147483647 minutes; the default is 30 minutes. The transfer interval is the same as the collection interval.</td>
</tr>
<tr>
<td>7</td>
<td>url primary URL</td>
<td>Specify the NMS (host) that the bulk-statistics file should be transferred to and the protocol to use for transfer (FTP, RCP, or TFTP). You also can optionally enter the url secondary command to specify a backup transfer destination.</td>
</tr>
<tr>
<td>8</td>
<td>retry number</td>
<td>(Optional) Specify the number of transmission retries. The range is from 1 to 100; the default is 0 (no retries).</td>
</tr>
<tr>
<td>9</td>
<td>retain minutes</td>
<td>(Optional) Specify how long the bulk-statistics file should be kept in system memory. The valid range is 0 to 20000 minutes; the default is 0 (the file is deleted immediately after a successful transfer).</td>
</tr>
<tr>
<td>10</td>
<td>enable</td>
<td>Begin the bulk-statistics data collection and transfer process for this configuration. You must enter this command to start periodic collection and transfer.</td>
</tr>
<tr>
<td>11</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>12</td>
<td>show mib bulk transfer</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>13</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Enter the **no enable** bulk statistics transfer configuration mode command to stop the collection process. Enter the **enable** command again to restart the operation. Every time you restart the process with the **enable** command, data is collected in a new bulk-statistics file.
This is an example of configuring the bulk-statistics transfer and enabling the collection process:

```
Switch(config)# snmp mib bulkstat transfer testtransfer
Switch(config-bulk-tr)# format schemaASCII
Switch(config-bulk-tr)# buffer-size 2147483647
Switch(config-bulk-tr)# schema testschemain
Switch(config-bulk-tr)# schema testschemain
Switch(config-bulk-tr)# transfer-interval 1
Switch(config-bulk-tr)# url primary tftp://host/folder/bulkstat1
Switch(config-bulk-tr)# retain 20
Switch(config-bulk-tr)# retry 2
Switch(config-bulk-tr)# enable
Switch(config-bulk-tr)# exit
```

Enter the `show snmp mib bulk transfer` privileged EXEC command to view the configured transfer operation.

### Configuring the Cisco Process MIB CPU Threshold Table

In Cisco IOS Release 12.2(37)SE and later, you can use the CLI to configure the Cisco Process MIB CPU threshold table.

**Note**


Beginning in privileged EXEC mode, follow these steps to configure a CPU threshold table:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>process cpu statistics limit entry-percentage number [size seconds]</td>
<td>Set the process entry limit and the size of the history table for CPU utilization statistics.</td>
</tr>
</tbody>
</table>

- For *entry-percentage number*, enter the percentage (1 to 100) of CPU utilization that a process must use to become part of the history table.
- (Optional) For *size seconds*, set the duration of time in seconds for which CPU statistics are stored in the history table. The range is from 5 to 86400 seconds; the default is 600.
Chapter 31      Configuring SNMP

SNMP Examples

This example shows how to enable all versions of SNMP. The configuration permits any SNMP manager to access all objects with read-only permissions using the community string "public." This configuration does not cause the switch to send any traps.

```
Switch(config)# snmp-server community public
```

This example shows how to permit any SNMP manager to access all objects with read-only permission using the community string "public." The switch also sends VTP traps to the hosts 192.180.1.111 and 192.180.1.33 using SNMPv1 and to the host 192.180.1.27 using SNMPv2C. The community string "public" is sent with the traps.

```
Switch(config)# snmp-server community public
Switch(config)# snmp-server enable traps vtp
Switch(config)# snmp-server host 192.180.1.27 version 2c public
Switch(config)# snmp-server host 192.180.1.111 version 1 public
Switch(config)# snmp-server host 192.180.1.33 public
```

This example shows how to allow read-only access for all objects to members of access list 4 that use the "comaccess" community string. No other SNMP managers have access to any objects. SNMP Authentication Failure traps are sent by SNMPv2C to the host cisco.com using the community string "public." 

```
Switch(config)# snmp-server community comaccess ro 4
Switch(config)# snmp-server enable traps snmp authentication
Switch(config)# snmp-server host cisco.com version 2c public
```

This example shows how to send Entity MIB traps to the host cisco.com. The community string is restricted. The first line enables the switch to send Entity MIB traps in addition to any traps previously enabled. The second line specifies the destination of these traps and overwrites any previous snmp-server host commands for the host cisco.com.

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

This example shows how to enable the switch to send all traps to the host myhost.cisco.com using the community string public:
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server host myhost.cisco.com public

This example shows how to associate a user with a remote host and to send auth (authNoPriv) authentication-level informs when the user enters global configuration mode:
Switch(config)# snmp-server engineID remote 192.180.1.27 0000006300100a1c0b4011b
Switch(config)# snmp-server group authgroup v3 auth
Switch(config)# snmp-server user authuser authgroup remote 192.180.1.27 v3 auth md5
mypassword
Switch(config)# snmp-server user authuser authgroup v3 auth md5 mypassword
Switch(config)# snmp-server host 192.180.1.27 informs version 3 auth authuser config
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server inform retries 0

This example shows how to enable SNMP notifications to provide information on the transfer status of the periodic MIB data collection and transfer mechanism (bulk statistics):
Switch(config)# snmp-server enable traps bulkstat
Switch(config)# snmp-server host 192.180.1.27 informs version 2 public bulkstat

This example shows how to enable SNMP notifications to provide information on the Cisco Process MIB CPU threshold table:
Switch(config)# snmp-server enable traps cpu threshold
Switch(config)# snmp-server host 192.180.1.27 informs version 2 public cpu

### Displaying SNMP Status

To display SNMP input and output statistics, including the number of illegal community string entries, errors, and requested variables, use the `show snmp` privileged EXEC command. You can also use the other privileged EXEC commands in Table 31-6 to display SNMP information. For information about the fields in the output displays, see the *Cisco IOS Configuration Fundamentals Command Reference, Release 12.2*.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>show snmp</td>
<td>Displays SNMP statistics.</td>
</tr>
<tr>
<td>show snmp engineID [local</td>
<td>Displays information on the local SNMP engine and all remote engines that have</td>
</tr>
<tr>
<td></td>
<td>remote]</td>
</tr>
<tr>
<td>show snmp group</td>
<td>Displays information on each SNMP group on the network.</td>
</tr>
<tr>
<td>show snmp mib bulk transfer</td>
<td>Displays transfer status of files generated by the Periodic MIB Data Collection</td>
</tr>
<tr>
<td></td>
<td>and Transfer Mechanism (bulk statistics feature).</td>
</tr>
<tr>
<td>show snmp pending</td>
<td>Displays information on pending SNMP requests.</td>
</tr>
</tbody>
</table>
### Table 31-6 Commands for Displaying SNMP Information

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>show snmp sessions</td>
<td>Displays information on the current SNMP sessions.</td>
</tr>
<tr>
<td>show snmp user</td>
<td>Displays information on each SNMP user name in the SNMP users table.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> You must use this command to display SNMPv3 configuration information for auth</td>
</tr>
</tbody>
</table>
Displaying SNMP Status
Configuring Embedded Event Manager

Embedded Event Manager (EEM) is a distributed and customized approach to event detection and recovery within a Cisco IOS device. EEM offers the ability to monitor events and take informational, corrective, or any other EEM action when the monitored events occur or when a threshold is reached. An EEM policy defines an event and the actions to be taken when that event occurs.

This chapter tells how to use EEM and how to configure it on the Catalyst 3750 Metro switch. For complete syntax and usage information for the commands used in this chapter, see the switch command reference for this release and the Cisco IOS Network Management Command Reference. For the complete EEM document set, see these documents in the Cisco IOS Network Management Configuration Guide:

- Embedded Event Manager Overview
- Writing Embedded Event Manager Policies Using the Cisco IOS CLI
- Writing Embedded Event Manager Policies Using Tcl

This chapter includes these sections:

- Understanding Embedded Event Manager, page 32-1
- Configuring Embedded Event Manager, page 32-6
- Displaying Embedded Event Manager Information, page 32-7

Understanding Embedded Event Manager

EEM monitors key system events and then acts on them through a set policy. This policy is a programmed script that you can use to customize a script to invoke an action based on a given set of events occurring. The script generates actions such as generating custom syslog or Simple Network Management Protocol (SNMP) traps, invoking CLI commands, forcing a failover, and so forth. The event management capabilities of EEM are useful because not all event management can be managed from the switch and because some problems compromise communication between the switch and the external network management device. Network availability is improved if automatic recovery actions are performed without rebooting the switch,
Figure 32-1 shows the relationship between the EEM server, the core event publishers (event detectors), and the event subscribers (policies). The event publishers screen events and when there is a match on an event specification that is provided by the event subscriber. Event detectors notify the EEM server when an event occurs. The EEM policies then implement recovery based on the current state of the system and the actions specified in the policy for the given event.

Figure 32-1  Embedded Event Manager Core Event Detectors

See the EEM Configuration for Cisco Integrated Services Router Platforms Guide for examples of EEM deployment.

These sections contain this conceptual information:

- Event Detectors, page 32-3
- Embedded Event Manager Actions, page 32-4
- Embedded Event Manager Policies, page 32-4
- Embedded Event Manager Environment Variables, page 32-5
- EEM 3.2, page 32-5
Event Detectors

EEM software programs known as event detectors determine when an EEM event occurs. Event detectors are separate systems that provide an interface between the agent being monitored, for example SNMP, and the EEM policies where an action can be implemented.

EEM allows these event detectors:

- Application-specific event detector—Allows any EEM policy to publish an event.
- IOS CLI event detector—Generates policies based on the commands entered through the CLI.
- Generic Online Diagnostics (GOLD) event detector—Publishes an event when a GOLD failure event is detected on a specified card and subcard.
- Counter event detector—Publishes an event when a named counter crosses a specified threshold.
- Interface counter event detector—Publishes an event when a generic Cisco IOS interface counter for a specified interface crosses a defined threshold. A threshold can be specified as an absolute value or an incremental value. For example, if the incremental value is set to 50, an event would be published when the interface counter increases by 50.
  This detector also publishes an event about an interface based on the rate of change for the entry and exit values.
- None event detector—Publishes an event when the event manager run CLI command executes an EEM policy. EEM schedules and runs policies on the basis on an event specification within the policy itself. An EEM policy must be manually identified and registered before the event manager run command executes.
- Online insertion and removal event detector—Publishes an event when a hardware insertion or removal (OIR) event occurs.
- Remote procedure call (RPC) event detector—Invokes EEM policies from outside the switch over an encrypted connecting using Secure Shell (SSH) and uses Simple Object Access Protocol (SOAP) data encoding for exchanging XML-based messages. It also runs EEM policies and then gets the output in a SOAP XML-formatted reply.
- SNMP event detector—Allows a standard SNMP MIB object to be monitored and an event to be generated when
  - The object matches specified values or crosses specified thresholds.
  - The SNMP delta value, the difference between the monitored Object Identifier (OID) value at the beginning the period and the actual OID value when the event is published, matches a specified value.
- SNMP notification event detector—Intercepts SNMP trap and inform messages received by the switch. The event is generated when an incoming message matches a specified value or crosses a defined threshold.
- Syslog event detector—Allows for screening syslog messages for a regular expression pattern match. The selected messages can be further qualified, requiring that a specific number of occurrences be logged within a specified time. A match on a specified event criteria triggers a configured policy action.
- Timer event detector—Publishes events for
  - An absolute-time-of-day timer publishes an event when a specified absolute date and time occurs.
  - A countdown timer publishes an event when a timer counts down to zero.
Understanding Embedded Event Manager

- A watchdog timer publishes an event when a timer counts down to zero. The timer automatically resets itself to its initial value and starts to count down again.
- A CRON timer publishes an event by using a UNIX standard CRON specification to define when the event is to be published. A CRON timer never publishes events more than once per minute.

• Watchdog event detector (IOSWDSysMon) - Publishes an event when one of these events occurs:
  - CPU utilization for a Cisco IOS process crosses a threshold.
  - Memory utilization for a Cisco IOS process crosses a threshold.

Two events can be monitored at the same time, and the event publishing criteria requires that one or both events cross their specified thresholds.

Embedded Event Manager Actions

These actions occur in response to an event:
• Modifying a named counter.
• Publishing an application-specific event.
• Generating an SNMP trap.
• Generating prioritized syslog messages.
• Reloading the Cisco IOS software.

Embedded Event Manager Policies

EEM can monitor events and provide information, or take corrective action when the monitored events occur or a threshold is reached. An EEM policy is an entity that defines an event and the actions to be taken when that event occurs.

There are two types of EEM policies: an applet or a script. An applet is a simple policy that is defined within the CLI configuration. It is a concise method for defining event screening criteria and the actions to be taken when that event occurs. Scripts are defined on the networking device by using an ASCII editor. The script is then copied to the networking device and registered with EEM.

You use EEM to write and implement your own policies using the EEM policy tool command language (TCL) script.

Cisco enhancements to TCL in the form of keyword extensions facilitate the development of EEM policies. These keywords identify the detected event, the subsequent action, utility information, counter values, and system information.

For complete information on configuring EEM policies and scripts, see the Cisco IOS Network Management Configuration Guide, Release 12.4T.
Embedded Event Manager Environment Variables

EEM uses environment variables in EEM policies. These variables are defined in a EEM policy tool command language (TCL) script by running a CLI command and the event manager environment command. These environment variables can be defined in EEM:

- **User-defined variables**
  Defined by the user for a user-defined policy.

- **Cisco-defined variables**
  Defined by Cisco for a specific sample policy.

- **Cisco built-in variables (available in EEM applets)**
  Defined by Cisco and can be read-only or read-write. The read-only variables are set by the system before an applet starts to execute. The single read-write variable, _exit_status, allows you to set the exit status for policies triggered from synchronous events.

Cisco-defined environment variables and Cisco system-defined environment variables might apply to one specific event detector or to all event detectors. Environment variables that are user-defined or defined by Cisco in a sample policy are set by using the event manager environment global configuration command. You must defined the variables in the EEM policy before you register the policy.

For information about the environmental variables that EEM supports, see the Cisco IOS Network Management Configuration Guide, Release 12.4T.

EEM 3.2

EEM 3.2 is supported in Cisco IOS Release 12.2(52)SE and later and introduces these event detectors:

- **Neighbor Discovery**—Neighbor Discovery event detector provides the ability to publish a policy to respond to automatic neighbor detection when:
  - a Cisco Discovery Protocol (CDP) cache entry is added, deleted, or updated.
  - a Link Layer Discovery Protocol (LLDP) cache entry is added, deleted or updated.
  - an interface link status changes.
  - an interface line status changes.

- **Identity**—Identity event detector generates an event when AAA authorization and authentication is successful, when failure occurs, or after normal user traffic on the port is allowed to flow.

- **Mac-Address-Table**—Mac-Address-Table event detector generates an event when a MAC address is learned in the MAC address table.

**Note**

The Mac-Address-Table event detector is supported only on switch platforms and can be used only on Layer 2 interfaces where MAC addresses are learned. Layer 3 interfaces do not learn addresses, and routers do not usually support the MAC address-table infrastructure needed to notify EEM of a learned MAC address.

EEM 3.2 also introduces CLI commands to support the applets to work with the new event detectors. For further details about EEM 3.2 features, see the Embedded Event Manager 3.2 document.

## Configuring Embedded Event Manager

These sections contain this configuration information:

- Registering and Defining an Embedded Event Manager Applet, page 32-6
- Registering and Defining an Embedded Event Manager TCL Script, page 32-7

For complete information about configuring embedded event manager, see the Cisco IOS Network Management Configuration Guide, Release 12.4T.

### Registering and Defining an Embedded Event Manager Applet

Beginning in privileged EXEC mode, perform this task to register an applet with EEM and to define the EEM applet using the event applet and action applet configuration commands.

**Note**

Only one event applet command is allowed in an EEM applet. Multiple action applet commands are permitted. If you do not specify the no event and no action commands, the applet is removed when you exit configuration mode.

#### Command Purpose

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>event manager applet applet-name</td>
<td>Register the applet with EEM and enter applet configuration mode.</td>
</tr>
<tr>
<td>3</td>
<td>event snmp oid oid-value get-type {exact</td>
<td>next} entry-op {gt</td>
</tr>
<tr>
<td>4</td>
<td>action label syslog [priority priority-level] msg msg-text</td>
<td>Specify the action when an EEM applet is triggered. Repeat this action to add other CLI commands to the applet. (Optional) The priority keyword specifies the priority level of the syslog messages. If selected, you need to define the priority-level argument. For msg-text, the argument can be character text, an environment variable, or a combination of the two.</td>
</tr>
<tr>
<td>5</td>
<td>end</td>
<td>Exit applet configuration mode and return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

This example shows the output for EEM when one of the fields specified by an SNMP object ID crosses a defined threshold:

Switch(config-applet)# event snmp oid 1.3.6.1.4.1.9.9.48.1.1.1.6.1 get-type exact entry-op lt entry-val 5120000 poll-interval 10

These examples show actions that are taken in response to an EEM event:

Switch(config-applet)# action 1.0 syslog priority critical msg "Memory exhausted; current available memory is $_snmp_oid_val bytes"

Switch (config-applet)# action 2.0 force-switchover
Registering and Defining an Embedded Event Manager TCL Script

Beginning in privileged EXEC mode, perform this task to register a TCL script with EEM and to define the TCL script and policy commands.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 1</td>
<td>show event manager environment [all</td>
</tr>
<tr>
<td></td>
<td>variable-name]</td>
</tr>
<tr>
<td></td>
<td>]</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 3</td>
<td>event manager environment variable-name string</td>
</tr>
<tr>
<td>Step 4</td>
<td>event manager policy policy-file-name [type system] [trap]</td>
</tr>
<tr>
<td>Step 5</td>
<td>exit</td>
</tr>
</tbody>
</table>

This example shows the sample output for the show event manager environment command:

```
Switch# show event manager environment all
No.  Name                       Value
1    _cron_entry                0-59/2 0-23/1 * * 0-6
2    _show_cmd                  show ver
3    _syslog_pattern            .*UPDOWN.*Ethernet1/0.*
4    _config_cmd1               interface Ethernet1/0
5    _config_cmd2               no shut
```

This example shows a CRON timer environment variable, which is assigned by the software, to be set to every second minute, every hour of every day:

```
Switch (config)# event manager environment_cron_entry 0-59/2 0-23/1 * * 0-6
```

This example shows the sample EEM policy named tm_cli_cmd.tcl registered as a system policy. The system policies are part of the Cisco IOS image. User-defined TCL scripts must first be copied to flash memory.

```
Switch (config)# event manager policy tm_cli_cmd.tcl type system
```

Displaying Embedded Event Manager Information

To display information about EEM, including EEM registered policies and EEM history data, see the Cisco IOS Network Management Command Reference.
Configuring Network Security with ACLs

This chapter describes how to configure network security on the Catalyst 3750 Metro switch by using access control lists (ACLs), which are also referred to in commands and tables as access lists.

Note

For complete syntax and usage information for the commands used in this chapter, see the command reference for this release, see the “Configuring IP Services” section in the “IP Addressing and Services” chapter of the Cisco IOS IP Configuration Guide, Release 12.2, and to these software configuration guides and command references:

- Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2
- Cisco IOS IP Command Reference, Volume 3 of 3: Multicast, Release 12.2

This chapter consists of these sections:

- Understanding ACLs, page 33-1
- Configuring IP ACLs, page 33-6
- Creating Named MAC Extended ACLs, page 33-27
- Configuring VLAN Maps, page 33-29
- Using VLAN Maps with Router ACLs, page 33-36
- Displaying ACL Configuration, page 33-40

Understanding ACLs

Packet filtering can help limit network traffic and restrict network use by certain users or devices. ACLs can filter traffic as it passes through a router or switch and permit or deny packets crossing specified interfaces or VLANs. An ACL is a sequential collection of permit and deny conditions that apply to packets. When a packet is received on an interface, the switch compares the fields in the packet against any applied ACLs to verify that the packet has the required permissions to be forwarded, based on the criteria specified in the access lists. It tests packets against the conditions in an access list one by one. The first match determines whether the switch accepts or rejects the packets. Because the switch stops testing conditions after the first match, the order of conditions in the list is critical. If no conditions match, the switch rejects the packets. If there are no restrictions, the switch forwards the packet; otherwise, the switch drops the packet. The switch can access-control all packets it switches, including packets bridged within a VLAN.
Understanding ACLs

You configure access lists on a router or Layer 3 switch to provide basic security for your network. If you do not configure ACLs, all packets passing through the switch could be allowed onto all parts of the network. You can use ACLs to control which hosts can access different parts of a network or to decide which types of traffic are forwarded or blocked at router interfaces. For example, you can allow e-mail traffic to be forwarded but not Telnet traffic. ACLs can be configured to block inbound traffic, outbound traffic, or both.

An ACL contains an ordered list of access control entries (ACEs). Each ACE specifies permit or deny and a set of conditions the packet must satisfy in order to match the ACE. The meaning of permit or deny depends on the context in which the ACL is used.

The switch supports IP ACLs and Ethernet (MAC) ACLs:
- IP ACLs filter IP traffic, including TCP, User Datagram Protocol (UDP), Internet Group Management Protocol (IGMP), and Internet Control Message Protocol (ICMP).
- Ethernet ACLs filter non-IPv4 traffic.

This switch also supports quality of service (QoS) classification ACLs. For more information, see the “Ingress Classification Based on QoS ACLs” section on page 34-11.

This section includes information on these topics:
- Supported ACLs, page 33-2
- Handling Fragmented and Unfragmented Traffic, page 33-5

Supported ACLs

The switch supports three applications of ACLs to filter traffic:
- Router ACLs access-control routed traffic between VLANs and are applied to Layer 3 interfaces.
- Port ACLs access-control traffic entering a Layer 2 interface. The switch does not support port ACLs in the outbound direction. You can apply only one IP access list and one MAC access list to a Layer 2 interface.
- VLAN ACLs or VLAN maps access-control all packets (bridged and routed). You can use VLAN maps to filter traffic between devices in the same VLAN. VLAN maps are configured to provide access-control based on Layer 3 addresses for IP. Unsupported protocols are access-controlled through MAC addresses using Ethernet ACEs. After a VLAN map is applied to a VLAN, all packets (routed or bridged) entering the VLAN are checked against the VLAN map. Packets can either enter the VLAN through a switch port or through a routed port after being routed.

You can use router ACLs, input port ACLs, and VLAN maps on the same switch. However, a port ACL takes precedence over a router ACL or VLAN map.
- When both an input port ACL and a VLAN map are applied, incoming packets received on ports with a port ACL applied are filtered by the port ACL. Other packets are filtered by the VLAN map.
- When an input router ACL and input port ACL exist in an switch virtual interface (SVI), incoming packets received on ports to which a port ACL is applied are filtered by the port ACL. Incoming routed IP packets received on other ports are filtered by the router ACL. Other packets are not filtered.
- When an output router ACL and input port ACL exist in an SVI, incoming packets received on the ports to which a port ACL is applied are filtered by the port ACL. Outgoing routed IP packets are filtered by the router ACL. Other packets are not filtered.
When a VLAN map, input router ACL, and input port ACL exist in an SVI, incoming packets received on the ports to which a port ACL is applied are only filtered by the port ACL. Incoming routed IP packets received on other ports are filtered by both the VLAN map and the router ACL. Other packets are filtered only by the VLAN map.

When a VLAN map, output router ACL, and input port ACL exist in an SVI, incoming packets received on the ports to which a port ACL is applied are only filtered by the port ACL. Outgoing routed IP packets are filtered by both the VLAN map and the router ACL. Other packets are filtered only by the VLAN map.

**Router ACLs**

You can apply router ACLs on SVIs, which are Layer 3 interfaces to VLANs; on physical Layer 3 interfaces; and on Layer 3 EtherChannel interfaces. You apply router ACLs on interfaces for specific directions (inbound or outbound). You can apply one router ACL in each direction on an interface.

One ACL can be used with multiple features for a given interface, and one feature can use multiple ACLs. When a single router ACL is used by multiple features, it is examined multiple times.

- Standard IP access lists use source addresses for matching operations.
- Extended IP access lists use source and destination addresses and optional protocol type information for matching operations.

The switch examines ACLs associated with features configured on a given interface and a direction. As packets enter the switch on an interface, ACLs associated with all inbound features configured on that interface are examined. After packets are routed and before they are forwarded to the next hop, all ACLs associated with outbound features configured on the egress interface are examined.

ACLs permit or deny packet forwarding based on how the packet matches the entries in the ACL, and can be used to control access to a network or to part of a network. In Figure 33-1, ACLs applied at the switch input allow Host A to access the Human Resources network, but prevent Host B from accessing the same network.

**Figure 33-1 Using ACLs to Control Traffic to a Network**
Port ACLs

Port ACLs are ACLs that are applied to Layer 2 interfaces on a switch. Port ACLs are supported only on physical interfaces and not on EtherChannel interfaces. Port ACLs are applied only on interfaces for inbound traffic.

These access lists are supported on Layer 2 interfaces:

- Standard IP access lists using source addresses
- Extended IP access lists using source and destination addresses and optional protocol type information
- MAC extended access lists using source and destination MAC addresses and optional protocol type information

As with router ACLs, the switch examines ACLs associated with features configured on a given interface and permits or denies packet forwarding based on how the packet matches the entries in the ACL. ACLs can only be applied to Layer 2 interfaces in the inbound direction. In the example in Figure 33-1, if all workstations were in the same VLAN, ACLs applied at the Layer 2 input would allow Host A to access the Human Resources network, but prevent Host B from accessing the same network.

When you apply a port ACL to a trunk port, the ACL filters traffic on all VLANs present on the trunk port. When you apply a port ACL to a port with voice VLAN, the ACL filters traffic on both data and voice VLANs.

With port ACLs, you can filter IPv4 traffic by using IP access lists and non-IPv4 traffic by using MAC addresses. You can filter both IP and non-IP traffic on the same Layer 2 interface by applying both an IP access list and a MAC access list to the interface.

Note

You cannot apply more than one IP access list and one MAC access list to a Layer 2 interface. If an IP access list or MAC access list is already configured on a Layer 2 interface and you apply a new IP access list or MAC access list to the interface, the new ACL replaces the previously configured one.

VLAN Maps

VLAN ACLs or VLAN maps can access-control all traffic. You can apply VLAN maps to all packets that are routed into or out of a VLAN or are bridged within a VLAN. VLAN maps are used for security packet filtering. VLAN maps are not defined by direction (input or output).

You can configure VLAN maps to match Layer 3 addresses for IP traffic. All non-IPv4 protocols are access-controlled through MAC addresses and Ethertype using MAC VLAN maps. (IP traffic is not access controlled by MAC VLAN maps.) You can enforce VLAN maps only on packets going through the switch; you cannot enforce VLAN maps on traffic between hosts on a hub or on another switch connected to this switch.

With VLAN maps, forwarding of packets is permitted or denied, based on the action specified in the map. Figure 33-2 illustrates how a VLAN map is applied to deny a specific type of traffic from Host A in VLAN 10 from being forwarded. You can apply only one VLAN map to a VLAN.
Handling Fragmented and Unfragmented Traffic

IP packets can be fragmented as they cross the network. When this happens, only the fragment containing the beginning of the packet contains the Layer 4 information, such as TCP or UDP port numbers, ICMP type and code, and so on. All other fragments are missing this information.

Some ACEs do not check Layer 4 information and therefore can be applied to all packet fragments. ACEs that do test Layer 4 information cannot be applied in the standard manner to most of the fragments in a fragmented IP packet. When the fragment contains no Layer 4 information and the ACE tests some Layer 4 information, the matching rules are modified:

- Permit ACEs that check the Layer 3 information in the fragment (including protocol type, such as TCP, UDP, and so on) are considered to match the fragment regardless of what the missing Layer 4 information might have been.
- Deny ACEs that check Layer 4 information never match a fragment unless the fragment contains Layer 4 information.

Consider access list 102, configured with these commands, applied to three fragmented packets:

```
Switch(config)# access-list 102 permit tcp any host 10.1.1.1 eq smtp
Switch(config)# access-list 102 deny tcp any host 10.1.1.2 eq telnet
Switch(config)# access-list 102 permit tcp any host 10.1.1.2
Switch(config)# access-list 102 deny tcp any any
```

In the first and second ACEs in the examples, the `eq` keyword after the destination address means to test for the TCP-destination-port well-known numbers equaling Simple Mail Transfer Protocol (SMTP) and Telnet, respectively.

- Packet A is a TCP packet from host 10.2.2.2, port 65000, going to host 10.1.1.1 on the SMTP port. If this packet is fragmented, the first fragment matches the first ACE (a permit) as if it were a complete packet because all Layer 4 information is present. The remaining fragments also match the first ACE, even though they do not contain the SMTP port information, because the first ACE only checks Layer 3 information when applied to fragments. The information in this example is that the packet is TCP and that the destination is 10.1.1.1.
- Packet B is from host 10.2.2.2, port 65001, going to host 10.1.1.2 on the Telnet port. If this packet is fragmented, the first fragment matches the second ACE (a deny) because all Layer 3 and Layer 4 information is present. The remaining fragments in the packet do not match the second ACE because they are missing Layer 4 information. Instead, they match the third ACE (a permit).
Because the first fragment was denied, host 10.1.1.2 cannot reassemble a complete packet, so packet B is effectively denied. However, the later fragments that are permitted will consume bandwidth on the network and resources of host 10.1.1.2 as it tries to reassemble the packet.

- Fragmented packet C is from host 10.2.2.2, port 65001, going to host 10.1.1.3, port ftp. If this packet is fragmented, the first fragment matches the fourth ACE (a deny). All other fragments also match the fourth ACE because that ACE does not check any Layer 4 information and because Layer 3 information in all fragments shows that they are being sent to host 10.1.1.3, and the earlier permit ACEs were checking different hosts.

## Configuring IP ACLs

Configuring IP ACLs on the switch is the same as configuring IP ACLs on other Cisco switches and routers. The process is briefly described here. For more detailed information on configuring ACLs, see the “Configuring IP Services” section in the “IP Addressing and Services” chapter of the *Cisco IOS IP Configuration Guide, Release 12.2*. For detailed information about the commands, see these documents:

- *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2*
- *Cisco IOS IP Command Reference, Volume 3 of 3: Multicast, Release 12.2*

The switch does not support these IOS router ACL-related features:

- Non-IPv4 protocol ACLs (see Table 33-1 on page 33-7) or bridge-group ACLs
- IP accounting
- Inbound and outbound rate limiting (except with QoS ACLs)
- Reflexive ACLs or dynamic ACLs (except for some specialized dynamic ACLs used by the switch clustering feature)
- ACL logging for port ACLs and VLAN maps

These are the steps to use IP ACLs on the switch:

### Step 1
Create an ACL by specifying an access list number or name and access conditions.

### Step 2
Apply the ACL to interfaces or terminal lines. You can also apply standard and extended IP ACLs to VLAN maps.

This section includes the following information:

- Creating Standard and Extended IP ACLs, page 33-7
- Applying an IP ACL to a Terminal Line, page 33-18
- Applying an IP ACL to an Interface, page 33-19
- Hardware and Software Treatment of IP ACLs, page 33-21
- Troubleshooting ACLs, page 33-21
- IP ACL Configuration Examples, page 33-22
Creating Standard and Extended IP ACLs

This section describes IP ACLs. An ACL is a sequential collection of permit and deny conditions. The switch tests packets against the conditions in an access list one by one. The first match determines whether the switch accepts or rejects the packet. Because the switch stops testing conditions after the first match, the order of the conditions is critical. If no conditions match, the switch denies the packet.

The software supports these types of ACLs or access lists for IP:

- Standard IP access lists use source addresses for matching operations.
- Extended IP access lists use source and destination addresses for matching operations and optional protocol-type information for finer granularity of control.

These sections describe access lists and how to create them:

- Access List Numbers, page 33-7
- Creating a Numbered Standard ACL, page 33-8
- Creating a Numbered Extended ACL, page 33-9
- Resequencing ACEs in an ACL, page 33-14
- Creating Named Standard and Extended ACLs, page 33-14
- Using Time Ranges with ACLs, page 33-16
- Including Comments in ACLs, page 33-18

Access List Numbers

The number you use to denote your ACL shows the type of access list that you are creating. Table 33-1 lists the access-list number and corresponding access list type and shows whether or not they are supported in the switch. The switch supports IP standard and IP extended access lists, numbers 1 to 199 and 1300 to 2699.

<table>
<thead>
<tr>
<th>Access List Number</th>
<th>Type</th>
<th>Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>1–99</td>
<td>IP standard access list</td>
<td>Yes</td>
</tr>
<tr>
<td>100–199</td>
<td>IP extended access list</td>
<td>Yes</td>
</tr>
<tr>
<td>200–299</td>
<td>Protocol type-code access list</td>
<td>No</td>
</tr>
<tr>
<td>300–399</td>
<td>DECnet access list</td>
<td>No</td>
</tr>
<tr>
<td>400–499</td>
<td>XNS standard access list</td>
<td>No</td>
</tr>
<tr>
<td>500–599</td>
<td>XNS extended access list</td>
<td>No</td>
</tr>
<tr>
<td>600–699</td>
<td>AppleTalk access list</td>
<td>No</td>
</tr>
<tr>
<td>700–799</td>
<td>48-bit MAC address access list</td>
<td>No</td>
</tr>
<tr>
<td>800–899</td>
<td>IPX standard access list</td>
<td>No</td>
</tr>
<tr>
<td>900–999</td>
<td>IPX extended access list</td>
<td>No</td>
</tr>
<tr>
<td>1000–1099</td>
<td>IPX SAP access list</td>
<td>No</td>
</tr>
<tr>
<td>1100–1199</td>
<td>Extended 48-bit MAC address access list</td>
<td>No</td>
</tr>
<tr>
<td>1200–1299</td>
<td>IPX summary address access list</td>
<td>No</td>
</tr>
</tbody>
</table>
Creating a Numbered Standard ACL

Beginning in privileged EXEC mode, follow these steps to create a numbered standard ACL:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>access-list access-list-number [deny</td>
</tr>
<tr>
<td></td>
<td>Define a standard IP access list by using a source address and wildcard.</td>
</tr>
<tr>
<td></td>
<td>The access-list-number is a decimal number from 1 to 99 or 1300 to 1999.</td>
</tr>
<tr>
<td></td>
<td>Enter deny or permit to specify whether to deny or permit access if conditions are matched.</td>
</tr>
<tr>
<td></td>
<td>The source is the source address of the network or host from which the packet is being sent specified as:</td>
</tr>
<tr>
<td></td>
<td>- The 32-bit quantity in dotted-decimal format.</td>
</tr>
<tr>
<td></td>
<td>- The keyword any as an abbreviation for source and source-wildcard of 0.0.0.0 255.255.255.255. You do not need to enter a source-wildcard.</td>
</tr>
<tr>
<td></td>
<td>- The keyword host as an abbreviation for source and source-wildcard of source 0.0.0.0.</td>
</tr>
<tr>
<td></td>
<td>(Optional) The source-wildcard applies wildcard bits to the source.</td>
</tr>
<tr>
<td></td>
<td>(Optional) Enter log to cause an informational logging message about the packet that matches the entry to be sent to the console.</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
</tr>
<tr>
<td></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show access-lists [number</td>
</tr>
<tr>
<td></td>
<td>Show the access list configuration.</td>
</tr>
<tr>
<td>Step 5</td>
<td>copy running-config startup-config</td>
</tr>
<tr>
<td></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Use the **no access-list access-list-number** global configuration command to delete the entire ACL. You cannot delete individual ACEs from numbered access lists.
When creating an ACL, remember that, by default, the end of the ACL contains an implicit deny statement for all packets that it did not find a match for before reaching the end. With standard access lists, if you omit the mask from an associated IP host address ACL specification, 0.0.0.0 is assumed to be the mask.

This example shows how to create a standard ACL to deny access to IP host 171.69.198.102, permit access to any others, and display the results.

```
Switch (config)# access-list 2 deny host 171.69.198.102
Switch (config)# access-list 2 permit any
Switch(config)# end
Switch# show access-lists
Standard IP access list 2
   10 deny    171.69.198.102
   20 permit any
```

The switch always rewrites the order of standard access lists so that entries with host matches and entries with matches having a don’t care mask of 0.0.0.0 are moved to the top of the list, above any entries with non-zero don’t care masks. Therefore, in show command output and in the configuration file, the ACEs do not necessarily appear in the order in which they were entered.

The switch software can provide logging messages about packets permitted or denied by a standard IP access list. That is, any packet that matches the ACL causes an informational logging message about the packet to be sent to the console. The level of messages logged to the console is controlled by the logging console commands controlling the syslog messages.

```
Because routing is done in hardware and logging is done in software, if a large number of packets match a permit or deny ACE containing a log keyword, the software might not be able to match the hardware processing rate, and not all packets will be logged.
```

The first packet that triggers the ACL causes a logging message right away, and subsequent packets are collected over 5-minute intervals before they are displayed or logged. The logging message includes the access list number, whether the packet was permitted or denied, the source IP address of the packet, and the number of packets from that source permitted or denied in the prior 5-minute interval.

After creating a numbered standard IP ACL, you can apply it to terminal lines (see the “Applying an IP ACL to a Terminal Line” section on page 33-18), to interfaces (see the “Applying an IP ACL to an Interface” section on page 33-19), or to VLANs (see the “Configuring VLAN Maps” section on page 33-29).

**Creating a Numbered Extended ACL**

Although standard ACLs use only source addresses for matching, you can use extended ACL source and destination addresses for matching operations and optional protocol type information for finer granularity of control. When you are creating ACEs in numbered extended access lists, remember that after you create the ACL, any additions are placed at the end of the list. You cannot reorder the list or selectively add or remove ACEs from a numbered list.

Some protocols also have specific parameters and keywords that apply to that protocol.

These IP protocols are supported (protocol keywords are in parentheses in bold):

- Authentication Header Protocol (**ahp**)
- Enhanced Interior Gateway Routing Protocol (**eigrp**)
- Encapsulation Security Payload (**esp**)
- generic routing encapsulation (**gre**)
- Internet Control Message Protocol (**icmp**)
- Internet Group Management Protocol (**igmp**)
- Interior Gateway Routing Protocol
(igrp), any Interior Protocol (ip), IP in IP tunneling (ipinip), KA9Q NOS-compatible IP over IP tunneling (nos), Open Shortest Path First routing (ospf), Payload Compression Protocol (pcp), Protocol Independent Multicast (pim), Transmission Control Protocol (tcp), or User Datagram Protocol (udp).

**Note**
ICMP echo-reply cannot be filtered. All other ICMP codes or types can be filtered.

For more details on the specific keywords for each protocol, see these software configuration guides and command references:

- *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2*
- *Cisco IOS IP Command Reference, Volume 3 of 3: Multicast, Release 12.2*

**Note**
The switch does not support dynamic or reflexive access lists. It also does not support filtering based on the type of service (ToS) minimize-monetary-cost bit.

Supported parameters can be grouped into these categories: TCP, UDP, ICMP, IGMP, or other IP.
Beginning in privileged EXEC mode, follow these steps to create an extended ACL:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2a</td>
<td>access-list access-list-number { deny</td>
</tr>
</tbody>
</table>

**Note** If you enter a dscp value, you cannot enter tos or precedence. You can enter both a tos and a precedence value with no dscp.

Define an extended IP access list and the access conditions.

The access-list-number is a decimal number from 100 to 199 or 2000 to 2699.

Enter deny or permit to specify whether to deny or permit the packet if conditions are matched.

For protocol, enter the name or number of an IP protocol: ahp, eigrp, esp, gre, icmp, igmp, igrp, ip, ipinip, nos, ospf, pcp, pim, tcp, or udp, or an integer in the range 0 to 255 representing an IP protocol number. To match any Internet protocol (including ICMP, TCP, and UDP) use the keyword ip.

**Note** This step includes options for most IP protocols. For additional specific parameters for TCP, UDP, ICMP, and IGMP, see steps 2b through 2e.

The source is the number of the network or host from which the packet is sent.

The source-wildcard applies wildcard bits to the source.

The destination is the network or host number to which the packet is sent.

The destination-wildcard applies wildcard bits to the destination.

Source, source-wildcard, destination, and destination-wildcard can be specified as:

- The 32-bit quantity in dotted-decimal format.
- The keyword any for 0.0.0.0 255.255.255.255 (any host).
- The keyword host for a single host 0.0.0.0.

The other keywords are optional and have these meanings:

- precedence—Enter to match packets with a precedence level specified as a number from 0 to 7 or by name: routine (0), priority (1), immediate (2), flash (3), flash-override (4), critical (5), internet (6), network (7).

- fragments—Enter to check non-initial fragments.

- tos—Enter to match by type of service level, specified by a number from 0 to 15 or a name: normal (0), max-reliability (2), max-throughput (4), min-delay (8).

- log—Enter to create an informational logging message to be sent to the console about the packet that matches the entry or log-input to include the input interface in the log entry.

- time-range—For an explanation of this keyword, see the “Using Time Ranges with ACLs” section on page 33-16.

- dscp—Enter to match packets with the DSCP value specified by a number from 0 to 63, or use the question mark (?) to see a list of available values.
## Configuring IP ACLs

### Command Format

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| `access-list access-list-number 
  (deny | permit) protocol any any 
  [precedence precedence] [tos tos] 
  [fragments] [log] [log-input] 
  [time-range time-range-name] 
  [dscp dscp]` | In access-list configuration mode, define an extended IP access list using an abbreviation for a source and source wildcard of 0.0.0.0 255.255.255.255 and an abbreviation for a destination and destination wildcard of 0.0.0.0 255.255.255.255. You can use the *any* keyword in place of source and destination address and wildcard. |

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| `access-list access-list-number 
  (deny | permit) protocol host host destination 
  [precedence precedence] [tos tos] 
  [fragments] [log] [log-input] 
  [time-range time-range-name] 
  [dscp dscp]` | Define an extended IP access list using an abbreviation for a source and source wildcard of *source* 0.0.0.0 and an abbreviation for a destination and destination wildcard of *destination* 0.0.0.0. You can use the *host* keyword in place of source and destination wildcard or mask. |

### Step 2b

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| `access-list access-list-number 
  (deny | permit) tcp source source-wildcard [operator port] 
  destination destination-wildcard [operator port] [established] 
  [precedence precedence] [tos tos] 
  [fragments] [log] [log-input] 
  [time-range time-range-name] 
  [dscp dscp] [flag]` | (Optional) Define an extended TCP access list and the access conditions. Enter *tcp* for Transmission Control Protocol. The parameters are the same as those described in Step 2a with these exceptions: (Optional) Enter an *operator* and *port* to compare source (if positioned after source source-wildcard) or destination (if positioned after destination destination-wildcard) port. Possible operators include *eq* (equal), *gt* (greater than), *lt* (less than), *neq* (not equal), and *range* (inclusive range). Operators require a port number (*range* requires two port numbers separated by a space). Enter the *port* number as a decimal number (from 0 to 65535) or the name of a TCP port. To see TCP port names, use the ? or see the “Configuring IP Services” section in the “IP Addressing and Services” chapter of the *Cisco IOS IP Configuration Guide, Release 12.2*. Use only TCP port numbers or names when filtering TCP. The additional optional keywords have these meanings: - **established**—Enter to match an established connection. This has the same function as matching on the *ack* or *rst* flag. - **flag**—Enter one of these flags to match by the specified TCP header bits: *ack* (acknowledge), *fin* (finish), *psh* (push), *rst* (reset), *syn* (synchronize), or *urg* (urgent). |

### Step 2c

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| `access-list access-list-number 
  (deny | permit) udp source source-wildcard [operator port] 
  destination destination-wildcard [operator port] [precedence precedence] 
  [tos tos] [fragments] [log] 
  [log-input] [time-range time-range-name] [dscp dscp]` | (Optional) Define an extended UDP access list and the access conditions. Enter *udp* for the User Datagram Protocol. The UDP parameters are the same as those described for TCP except that [operator *port*] port number or name must be a UDP port number or name, and the *flag* and *established* parameters are not valid for UDP. |
### Command

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>2d</td>
<td>access-list access-list-number {deny</td>
<td>permit} icmp source source-wildcard destination destination-wildcard [icmp-type</td>
</tr>
</tbody>
</table>
|      |         | (Optional) Define an extended ICMP access list and the access conditions. Enter icmp for Internet Control Message Protocol. The ICMP parameters are the same as those described for most IP protocols in Step 2a, with the addition of the ICMP message type and code parameters. These optional keywords have these meanings:  
- _icmp-type_—Enter to filter by ICMP message type, a number from 0 to 255.  
- _icmp-code_—Enter to filter ICMP packets that are filtered by ICMP message type by the ICMP message code, a number from 0 to 255.  
- _icmp-message_—Enter to filter ICMP packets by ICMP message type name or ICMP message type and code name. To see a list of ICMP message type names and ICMP message type and code names, use the ? or see the “Configuring IP Services” section of the _Cisco IOS IP Configuration Guide, Release 12.2_. |
| 2e   | access-list access-list-number \{deny | permit\} igmp source source-wildcard destination destination-wildcard [igmp-type] | [precedence precedence] | [tos tos] | [fragments] | [log] | [log-input] | [time-range time-range-name] | [dscp dscp] |
|      |         | (Optional) Define an extended IGMP access list and the access conditions. Enter igmp for Internet Group Management Protocol. The IGMP parameters are the same as those described for most IP protocols in Step 2a, with the addition of this optional parameter.  
- _igmp-type_—To match IGMP message type, enter a number from 0 to 15, or enter the message name (dvmrp, host-query, host-report, pim, or trace). |
| 3    | end     | Return to privileged EXEC mode. |
| 4    | show access-lists \[number | name\] | Verify the access list configuration. |
| 5    | copy running-config startup-config | (Optional) Save your entries in the configuration file. |

Use the no access-list _access-list-number_ global configuration command to delete the entire access list. You cannot delete individual ACEs from numbered access lists.

This example shows how to create and display an extended access list to deny Telnet access from any host in network 171.69.198.0 to any host in network 172.20.52.0 and permit any others. (The _eq_ keyword after the destination address means to test for the TCP destination port number equaling Telnet.)

```
Switch(config)# access-list 102 deny tcp 171.69.198.0 0.0.0.255 172.20.52.0 0.0.0.255 eq telnet
Switch(config)# access-list 102 permit tcp any any
Switch(config)# end
Switch# show access-lists
Extended IP access list 102
  10 deny tcp 171.69.198.0 0.0.0.255 172.20.52.0 0.0.0.255 eq telnet
  20 permit tcp any any
```

After an ACL is created, any additions (possibly entered from the terminal) are placed at the end of the list. You cannot selectively add or remove access list entries from a numbered access list.

**Note** When you are creating an ACL, remember that, by default, the end of the access list contains an implicit deny statement for all packets if it did not find a match before reaching the end.
After creating a numbered extended ACL, you can apply it to terminal lines (see the “Applying an IP ACL to a Terminal Line” section on page 33-18), to interfaces (see the “Applying an IP ACL to an Interface” section on page 33-19), or to VLANs (see the “Configuring VLAN Maps” section on page 33-29).

Resequencing ACEs in an ACL

In Cisco IOS Release 12.2(25)EY and later, sequence numbers for the entries in an access list are automatically generated when you create a new ACL. You can use the `ip access-list resequence` global configuration command to edit the sequence numbers in an ACL and change the order in which ACEs are applied. For example, if you add a new ACE to an ACL, it is placed at the bottom of the list. By changing the sequence number, you can move the ACE to a different position in the ACL.

For more information about the `ip access-list resequence` command, see this URL:


Creating Named Standard and Extended ACLs

You can identify IP ACLs with an alphanumeric string (a name) rather than a number. You can use named ACLs to configure more IP access lists in a router than if you were to use numbered access lists. If you identify your access list with a name rather than a number, the mode and command syntax are slightly different. However, not all commands that use IP access lists accept a named access list.

- The name you give to a standard or extended ACL can also be a number in the supported range of access list numbers. That is, the name of a standard IP ACL can be 1 to 99; the name of an extended IP ACL can be 100 to 199. The advantage of using named ACLs instead of numbered lists is that you can delete individual entries from a named list.

Consider these guidelines and limitations before configuring named ACLs:

- Not all commands that accept a numbered ACL accept a named ACL. ACLs for packet filters and route filters on interfaces can use a name. VLAN maps also accept a name.
- A standard ACL and an extended ACL cannot have the same name.
- Numbered ACLs are also available, as described in the “Creating Standard and Extended IP ACLs” section on page 33-7.
- You can use standard and extended ACLs (named or numbered) in VLAN maps.

Beginning in privileged EXEC mode, follow these steps to create a standard ACL using names:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>ip access-list standard name</code></td>
<td>Define a standard IP access list using a name, and enter access-list configuration mode.</td>
</tr>
</tbody>
</table>

**Note** The name can be a number from 1 to 99.
To remove a named standard ACL, use the **no ip access-list standard name** global configuration command.

Beginning in privileged EXEC mode, follow these steps to create an extended ACL using names:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>ip access-list extended name</td>
<td>Define an extended IP access list using a name and enter access-list configuration mode. <strong>Note</strong> The name can be a number from 100 to 199.</td>
</tr>
</tbody>
</table>
| 3    | deny {source [source-wildcard] | host source | any} [log] or permit {source [source-wildcard] | host source | any} [log] | In access-list configuration mode, specify one or more conditions denied or permitted to determine if the packet is forwarded or dropped.  
  - host source—A source and source wildcard of source 0.0.0.0.  
  - any—A source and source wildcard of 0.0.0.0 255.255.255.255. |
| 4    | end | Return to privileged EXEC mode. |
| 5    | show access-lists [number | name] | Show the access list configuration. |
| 6    | copy running-config startup-config | (Optional) Save your entries in the configuration file. |

To remove a named extended ACL, use the **no ip access-list extended name** global configuration command.

When you are creating standard extended ACLs, remember that, by default, the end of the ACL contains an implicit deny statement for everything if it did not find a match before reaching the end. For standard ACLs, if you omit the mask from an associated IP host address access list specification, 0.0.0.0 is assumed to be the mask.
After you create an ACL, any additions are placed at the end of the list. You cannot selectively add ACL entries to a specific ACL. However, you can use `no permit` and `no deny` access-list configuration mode commands to remove entries from a named ACL. This example shows how you can delete individual ACEs from the named access list `border-list`:

```
Switch(config)# ip access-list extended border-list
Switch(config-ext-nacl)# no permit ip host 10.1.1.3 any
```

Being able to selectively remove lines from a named ACL is one reason you might use named ACLs instead of numbered ACLs.

After creating a named ACL, you can apply it to interfaces (see the “Applying an IP ACL to an Interface” section on page 33-19) or VLANs (see the “Configuring VLAN Maps” section on page 33-29).

### Using Time Ranges with ACLs

You can selectively apply extended ACLs based on the time of day and week by using the `time-range` global configuration command. First, define a time-range name and set the times and the dates or the days of the week in the time range. Then enter the time-range name when applying an ACL to set restrictions to the access list. You can use the time range to define when the permit or deny statements in the ACL are in effect, for example, during a specified time period or on specified days of the week. The `time-range` keyword and argument are referenced in the named and numbered extended ACL task tables in the previous sections, the “Creating Standard and Extended IP ACLs” section on page 33-7, and the “Creating Named Standard and Extended ACLs” section on page 33-14.

These are some of the many possible benefits of using time ranges:

- You have more control over permitting or denying a user access to resources, such as an application (identified by an IP address/mask pair and a port number).
- You can control logging messages. ACL entries can be set to log traffic only at certain times of the day. Therefore, you can simply deny access without needing to analyze many logs generated during peak hours.

Time-based access lists trigger CPU activity because the new configuration of the access list must be merged with other features and the combined configuration loaded into the TCAM. For this reason, you should be careful not to have several access lists configured to take affect in close succession (within a small number of minutes of each other.)

---

**Note**

The time range relies on the switch system clock; therefore, you need a reliable clock source. We recommend that you use Network Time Protocol (NTP) to synchronize the switch clock. For more information, see the “Managing the System Time and Date” section on page 5-1.

Beginning in privileged EXEC mode, follow these steps to configure an time-range parameter for an ACL:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>time-range time-range-name</code></td>
<td>Assign a meaningful name (for example, workhours) to the time range to be created, and enter time-range configuration mode. The name cannot contain a space or quotation mark and must begin with a letter.</td>
</tr>
</tbody>
</table>
Chapter 33 Configuring Network Security with ACLs

Configuring IP ACLs

Repeat the steps if you have multiple items that you want in effect at different times.

To remove a configured time-range limitation, use the `no time-range time-range-name` global configuration command.

This example shows how to configure time ranges for workhours and for a January 1, 2005 holiday and to verify your configuration.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
</tr>
</thead>
</table>
| 3    | `absolute [start time date]`  
|      | `[end time date]`  
|      | or `periodic day-of-the-week hh:mm to [day-of-the-week] hh:mm`  
|      | or `periodic {weekdays | weekend | daily} hh:mm to hh:mm`  
|      | Specify when the function it will be applied to is operational.  
|      | • You can use only one `absolute` statement in the time range. If you configure more than one absolute statement, only the one configured last is executed.  
|      | • You can enter multiple `periodic` statements. For example, you could configure different hours for weekdays and weekends. |
| 4    | `end`  
|     | Return to privileged EXEC mode. |
| 5    | `show time-range`  
|     | Verify the time-range configuration. |
| 6    | `copy running-config startup-config`  
|     | (Optional) Save your entries in the configuration file. |

Repeat the steps if you have multiple items that you want in effect at different times.

To remove a configured time-range limitation, use the `no time-range time-range-name` global configuration command.

This example shows how to configure time ranges for workhours and for a January 1, 2005 holiday and to verify your configuration.

```
Switch(config)# time-range workhours  
Switch(config-time-range)# periodic weekdays 8:00 to 12:00  
Switch(config-time-range)# periodic weekdays 13:00 to 17:00  
Switch(config-time-range)# exit  
Switch(config)# time-range new_year_day_2005  
Switch(config-time-range)# absolute start 00:00 1 Jan 2005 end 23:59 1 Jan 2005  
Switch(config-time-range)# end  
Switch# show time-range  
    time-range entry: new_year_day_2003 (inactive)  
          absolute start 00:00 01 January 2003 end 23:59 01 January 2003  
    time-range entry: workhours (inactive)  
          periodic weekdays 8:00 to 12:00  
          periodic weekdays 13:00 to 17:00
```

To apply a time-range, enter the time-range name in an extended ACL that can implement time ranges. This example shows how to create and verify extended access list 188 that denies TCP traffic from any source to any destination during the defined holiday times and permits all TCP traffic during work hours.

```
Switch(config)# access-list 188 deny tcp any any time-range new_year_day_2005  
Switch(config)# access-list 188 permit tcp any any time-range workhours  
Switch(config)# end  
Switch# show access-lists  
    Extended IP access list 188  
          10 deny tcp any any time-range new_year_day_2005 (inactive)  
          20 permit tcp any any time-range workhours (inactive)
```
This example uses named ACLs to permit and deny the same traffic.

```
Switch(config)# ip access-list extended deny_access
Switch(config-ext-nacl)# deny tcp any any time-range new_year_day_2005
Switch(config-ext-nacl)# exit
Switch(config)# ip access-list extended may_access
Switch(config-ext-nacl)# permit tcp any any time-range workhours
Switch(config-ext-nacl)# end
Switch# show ip access-lists
Extended IP access list deny_access
  10 deny tcp any any time-range new_year_day_2003 (inactive)
Extended IP access list may_access
  10 permit tcp any any time-range workhours (inactive)
```

### Including Comments in ACLs

You can use the `remark` keyword to include comments (remarks) about entries in any IP standard or extended ACL. The remarks make the ACL easier for you to understand and scan. Each remark line is limited to 100 characters.

The remark can go before or after a permit or deny statement. You should be consistent about where you put the remark so that it is clear which remark describes which permit or deny statement. For example, it would be confusing to have some remarks before the associated permit or deny statements and some remarks after the associated statements.

To include a comment for IP numbered standard or extended ACLs, use the `access-list access-list number remark remark` global configuration command. To remove the remark, use the `no` form of this command.

In this example, the workstation belonging to Jones is allowed access, and the workstation belonging to Smith is not allowed access:

```
Switch(config)# access-list 1 remark Permit only Jones workstation through
Switch(config)# access-list 1 permit 171.69.2.88
Switch(config)# access-list 1 remark Do not allow Smith workstation through
Switch(config)# access-list 1 deny 171.69.3.13
```

For an entry in a named IP ACL, use the `remark` access-list configuration command. To remove the remark, use the `no` form of this command.

In this example, the Jones subnet is not allowed to use outbound Telnet:

```
Switch(config)# ip access-list extended telnetting
Switch(config-ext-nacl)# remark Do not allow Jones subnet to telnet out
Switch(config-ext-nacl)# deny tcp host 171.69.2.88 any eq telnet
```

### Applying an IP ACL to a Terminal Line

You can use numbered ACLs to control access to one or more terminal lines. You cannot apply named ACLs to lines. You must set identical restrictions on all the virtual terminal lines because a user can attempt to connect to any of them.

For procedures for applying ACLs to interfaces, see the “Applying an IP ACL to an Interface” section on page 33-19. For applying ACLs to VLANs, see the “Configuring VLAN Maps” section on page 33-29.
Beginning in privileged EXEC mode, follow these steps to restrict incoming and outgoing connections between a virtual terminal line and the addresses in an ACL:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>line [console</td>
<td>vty] line-number</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• console—Specify the console terminal line. The console port is DCE.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• vty—Specify a virtual terminal for remote console access.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The line-number is the first line number in a contiguous group that you want to configure when the line type is specified. The range is from 0 to 16.</td>
</tr>
<tr>
<td>3</td>
<td>access-class access-list-number {in</td>
<td>out}</td>
</tr>
<tr>
<td>4</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>5</td>
<td>show running-config</td>
<td>Display the access list configuration.</td>
</tr>
<tr>
<td>6</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To remove an ACL from a terminal line, use the **no access-class access-list-number {in | out}** line configuration command.

### Applying an IP ACL to an Interface

This section describes how to apply IP ACLs to network interfaces. You can apply an ACL to either outbound or inbound Layer 3 interfaces. You can apply ACLs only to inbound Layer 2 interfaces. Note these guidelines:

- When controlling access to an interface, you can use a named or numbered ACL.
- If you apply an ACL to a Layer 2 interface that is a member of a VLAN, the Layer 2 (port) ACL takes precedence over an input Layer 3 ACL applied to the VLAN interface or a VLAN map applied to the VLAN. Incoming packets received on the Layer 2 port are always filtered by the port ACL.
- If you apply an ACL to a Layer 3 interface and routing is not enabled on the switch, the ACL only filters packets that are intended for the CPU, such as SNMP, Telnet, or web traffic. You do not have to enable routing to apply ACLs to Layer 2 interfaces.

**Note** By default, the router sends Internet Control Message Protocol (ICMP) unreachable messages when a packet is denied by an access group. These access-group denied packets are not dropped in hardware but are bridged to the switch CPU so that it can generate the ICMP-unreachable message.
Beginning in privileged EXEC mode, follow these steps to control access to an interface:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Identify a specific interface for configuration, and enter interface</td>
</tr>
<tr>
<td></td>
<td>configuration mode.</td>
</tr>
<tr>
<td></td>
<td>The interface can be a Layer 2 interface (port ACL), or a Layer 3</td>
</tr>
<tr>
<td></td>
<td>interface (router ACL).</td>
</tr>
<tr>
<td>Step 3 ip access-group {access-list-number</td>
<td>Control access to the specified interface.</td>
</tr>
<tr>
<td>name} {in</td>
<td>out}</td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5 show running-config</td>
<td>Display the access list configuration.</td>
</tr>
<tr>
<td>Step 6 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To remove the specified access group, use the **no ip access-group {access-list-number | name} {in | out}** interface configuration command.

This example shows how to apply access list 2 on an interface to filter packets entering the interface:

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# ip access-group 2 in
```

**Note** When you apply the **ip access-group** interface configuration command to a Layer 3 interface (an SVI, a Layer 3 EtherChannel, or a routed port), the interface must have been configured with an IP address. Layer 3 access groups filter packets that are routed or are received by Layer 3 processes on the CPU. They do not affect packets bridged within a VLAN.

For inbound ACLs, after receiving a packet, the switch checks the packet against the ACL. If the ACL permits the packet, the switch continues to process the packet. If the ACL rejects the packet, the switch discards the packet.

For outbound ACLs, after receiving and routing a packet to a controlled interface, the switch checks the packet against the ACL. If the ACL permits the packet, the switch sends the packet. If the ACL rejects the packet, the switch discards the packet.

By default, the input interface sends ICMP Unreachable messages whenever a packet is discarded, regardless of whether the packet was discarded because of an ACL on the input interface or because of an ACL on the output interface. ICMP Unreachables are normally limited to no more than one every one-half second per input interface, but this can be changed by using the **ip icmp rate-limit unreachable** global configuration command.

When you apply an undefined ACL to an interface, the switch acts as if the ACL has not been applied to the interface and permits all packets. Remember this behavior if you use undefined ACLs for network security.
Hardware and Software Treatment of IP ACLs

ACL processing is primarily accomplished in hardware, but requires forwarding of some traffic flows to the CPU for software processing. If the hardware reaches its capacity to store ACL configurations, packets are sent to the CPU for forwarding. The forwarding rate for software-forwarded traffic is substantially less than for hardware-forwarded traffic.

For router ACLs, other factors can cause packets to be sent to the CPU:

- Using the log keyword
- Generating ICMP unreachable messages

When traffic flows are both logged and forwarded, forwarding is done by hardware, but logging must be done by software. Because of the difference in packet handling capacity between hardware and software, if the sum of all flows being logged (both permitted flows and denied flows) is of great enough bandwidth, not all of the packets that are forwarded can be logged.

If router ACL configuration cannot be applied in hardware, packets arriving in a VLAN that must be routed are routed in software, but are bridged in hardware. If ACLs cause large numbers of packets to be sent to the CPU, the switch performance can be negatively affected.

When you enter the `show ip access-lists` privileged EXEC command, the match count displayed does not account for packets that are access controlled in hardware. Use the `show access-lists hardware counters` privileged EXEC command to obtain some basic hardware ACL statistics for switched and routed packets.

Router ACLs function as follows:

- The hardware controls permit and deny actions of standard and extended ACLs (input and output) for security access control.
- If log has not been specified, the flows that match a deny statement in a security ACL are dropped by the hardware if ip unreachables is disabled. The flows matching a permit statement are switched in hardware.
- Adding the log keyword to an ACE in a router ACL causes a copy of the packet to be sent to the CPU for logging only. If the ACE is a permit statement, the packet is still switched and routed in hardware.

Troubleshooting ACLs

If this ACL manager message appears and [chars] is the access-list name,

`ACLMGR-2-NOVMR: Cannot generate hardware representation of access list [chars]`

The switch has insufficient resources to create a hardware representation of the ACL. The resources include hardware memory and label space but not CPU memory. A lack of available logical operation units or specialized hardware resources causes this problem. Logical operation units are needed for a TCP flag match or a test other than `eq` (ne, gt, lt, or range) on TCP, UDP, or SCTP port numbers.

Use one of these workarounds:

- Modify the ACL configuration to use fewer resources.
- Rename the ACL with a name or number that alphanumerically precedes the ACL names or numbers.
To determine the specialized hardware resources, enter the `show platform layer4 acl map` privileged EXEC command. If the switch does not have available resources, the output shows that index 0 to index 15 are not available.

For more information about configuring ACLs with insufficient resources, see CSCsq63926 in the Bug Toolkit.

For example, if you apply this ACL to an interface:

```
permit tcp source source-wildcard destination destination-wildcard range 5 60
permit tcp source source-wildcard destination destination-wildcard range 15 160
permit tcp source source-wildcard destination destination-wildcard range 115 1660
permit tcp source source-wildcard destination destination-wildcard
```

And if this message appears:

```
ACLMGR-2-NOVMR: Cannot generate hardware representation of access list [chars]
```

The flag-related operators are not available. To avoid this issue,

- Move the fourth ACE before the first ACE by using `ip access-list resequence` global configuration command:

```
permit tcp source source-wildcard destination destination-wildcard
permit tcp source source-wildcard destination destination-wildcard range 5 60
permit tcp source source-wildcard destination destination-wildcard range 15 160
permit tcp source source-wildcard destination destination-wildcard range 115 1660
```

or

- Rename the ACL with a name or number that alphanumerically precedes the other ACLs (for example, rename ACL 79 to ACL 1).

You can now apply the first ACE in the ACL to the interface. The switch allocates the ACE to available mapping bits in the Opselect index and then allocates flag-related operators to use the same bits in the TCAM.

### IP ACL Configuration Examples

This section provides examples of configuring and applying IP ACLs. For detailed information about compiling ACLs, see the *Cisco IOS Security Configuration Guide, Release 12.2* and to the Configuring IP Services” section in the “IP Addressing and Services” chapter of the *Cisco IOS IP Configuration Guide, Release 12.2*.

Figure 33-3 shows a small networked office environment with the routed Port 2 connected to Server A, containing benefits and other information that all employees can access, and routed Port 1 connected to Server B, containing confidential payroll data. All users can access Server A, but Server B has restricted access.

Use router ACLs to do this in one of two ways:

- Create a standard ACL, and filter traffic coming to the server from Port 1.
- Create an extended ACL, and filter traffic coming from the server into Port 1.
This example uses a standard ACL to filter traffic coming into Server B from an interface, permitting traffic only from Accounting’s source addresses 172.20.128.64 to 172.20.128.95. The ACL is applied to traffic coming out of routed Port 1 from the specified source address.

```
Switch(config)# access-list 6 permit 172.20.128.64 0.0.0.31
Switch(config)# end
Switch# show access-lists
Standard IP access list 6
  10 permit 172.20.128.64, wildcard bits 0.0.0.31
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip access-group 6 out
```

This example uses an extended ACL to filter traffic coming from Server B into Port 1, permitting traffic from any source address (in this case Server B) to only the Accounting destination addresses 172.20.128.64 to 172.20.128.95. The ACL is applied to traffic going into routed Port 1, permitting it to go only to the specified destination addresses. Note that with extended ACLs, you must enter the protocol (IP) before the source and destination information.

```
Switch(config)# access-list 106 permit ip any 172.20.128.64 0.0.0.31
Switch(config)# end
Switch# show access-lists
Extended IP access list 106
  10 permit ip any 172.20.128.64 0.0.0.31
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip access-group 106 in
```
Chapter 33  Configuring Network Security with ACLs

Numbered ACLs

In this example, network 36.0.0.0 is a Class A network whose second octet specifies a subnet; that is, its subnet mask is 255.255.0.0. The third and fourth octets of a network 36.0.0.0 address specify a particular host. Using access list 2, the switch accepts one address on subnet 48 and reject all others on that subnet. The last line of the list shows that the switch accepts addresses on all other network 36.0.0.0 subnets. The ACL is then applied to packets entering an interface.

```
Switch(config)# access-list 2 permit 36.48.0.3
Switch(config)# access-list 2 deny 36.48.0.0 0.0.255.255
Switch(config)# access-list 2 permit 36.0.0.0 0.255.255.255
```

Extended ACLs

In this example, the first line permits any incoming TCP connections with destination ports greater than 1023. The second line permits incoming TCP connections to the Simple Mail Transfer Protocol (SMTP) port of host 128.88.1.2. The third line permits incoming ICMP messages for error feedback.

```
Switch(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 gt 1023
Switch(config)# access-list 102 permit tcp any host 128.88.1.2 eq 25
Switch(config)# access-list 102 permit icmp any any
```

For another example of using an extended ACL, suppose that you have a network connected to the Internet, and you want any host on the network to be able to form TCP connections to any host on the Internet. However, you do not want IP hosts to be able to form TCP connections to hosts on your network, except to the mail (SMTP) port of a dedicated mail host.

SMTP uses TCP port 25 on one end of the connection and a random port number on the other end. The same port numbers are used throughout the life of the connection. Mail packets coming in from the Internet have a destination port of 25. Outbound packets have the port numbers reversed. Because the secure system of the network always accepts mail connections on port 25, the incoming and outgoing services are separately controlled. The ACL must be configured as an input ACL on the outbound interface and an output ACL on the inbound interface.

In this example, the network is a Class B network with the address 128.88.0.0, and the mail host address is 128.88.1.2. The `established` keyword is used only for the TCP to show an established connection. A match occurs if the TCP datagram has the ACK or RST bits set, which show that the packet belongs to an existing connection. The specified interface is the interface that connects the router to the Internet.

```
Switch(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 established
Switch(config)# access-list 102 permit tcp any host 128.88.1.2 eq 25
```

Named ACLs

This example creates a standard ACL named `internet_filter` and an extended ACL named `marketing_group`. The `internet_filter` ACL allows all traffic from the source address 1.2.3.4.

```
Switch(config)# ip access-list standard Internet_filter
Switch(config-ext-nacl)# permit 1.2.3.4
Switch(config-ext-nacl)# exit
```
The *marketing_group* ACL allows any TCP Telnet traffic to the destination address and wildcard 171.69.0.0 0.0.255.255 and denies any other TCP traffic. It permits ICMP traffic, denies UDP traffic from any source to the destination address range 171.69.0.0 through 179.69.255.255 with a destination port less than 1024, denies any other IP traffic, and provides a log of the result.

```plaintext
Switch(config)# ip access-list extended marketing_group
Switch(config-ext-nacl)# permit tcp any 171.69.0.0 0.0.255.255 eq telnet
Switch(config-ext-nacl)# deny tcp any any
Switch(config-ext-nacl)# permit icmp any any
Switch(config-ext-nacl)# deny udp any 171.69.0.0 0.0.255.255 lt 1024
Switch(config-ext-nacl)# deny ip any any log
Switch(config-ext-nacl)# exit
```

The ACLs are applied to an interface, which is configured as a Layer 3 port, with the *Internet_filter* ACL applied to outgoing traffic and the *marketing_group* ACL applied to incoming traffic.

```plaintext
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# no switchport
Switch(config-if)# ip address 2.0.5.1 255.255.255.0
Switch(config-if)# ip access-group Internet_filter out
Switch(config-if)# ip access-group marketing_group in
```

### Time Range Applied to an IP ACL

This example denies HTTP traffic on IP on Monday through Friday between the hours of 8:00 a.m. and 6:00 p.m (18:00). The example allows UDP traffic only on Saturday and Sunday from noon to 8:00 p.m. (20:00).

```plaintext
Switch(config)# time-range no-http
Switch(config)# periodic weekdays 8:00 to 18:00
!
Switch(config)# time-range udp-yes
Switch(config)# periodic weekend 12:00 to 20:00
!
Switch(config)# ip access-list extended strict
Switch(config-ext-nacl)# deny tcp any any eq www time-range no-http
Switch(config-ext-nacl)# permit udp any any time-range udp-yes
!
Switch(config-ext-nacl)# exit
Switch(config)# interface fastethernet1/0/1
Switch(config-if)# ip access-group strict in
```

### Commented IP ACL Entries

In this example of a numbered ACL, the workstation belonging to Jones is allowed access, and the workstation belonging to Smith is not allowed access:

```plaintext
Switch(config)# access-list 1 remark Permit only Jones workstation through
Switch(config)# access-list 1 permit 171.69.2.88
Switch(config)# access-list 1 remark Do not allow Smith workstation through
Switch(config)# access-list 1 deny 171.69.3.13
```

In this example of a numbered ACL, the Winter and Smith workstations are not allowed to browse the web:

```plaintext
Switch(config)# access-list 100 remark Do not allow Winter to browse the web
Switch(config)# access-list 100 deny host 171.69.3.85 any eq www
Switch(config)# access-list 100 remark Do not allow Smith to browse the web
Switch(config)# access-list 100 deny host 171.69.3.13 any eq www
```
In this example of a named ACL, the Jones subnet is not allowed access:

```
Switch(config)# ip access-list standard prevention
Switch(config-std-nacl)# remark Do not allow Jones subnet through
Switch(config-std-nacl)# deny 171.69.0.0 0.0.255.255
```

In this example of a named ACL, the Jones subnet is not allowed to use outbound Telnet:

```
Switch(config)# ip access-list extended telnetting
Switch(config-ext-nacl)# remark Do not allow Jones subnet to telnet out
Switch(config-ext-nacl)# deny tcp 171.69.0.0 0.0.255.255 any eq telnet
```

**ACL Logging**

Two variations of logging are supported on router ACLs. The `log` keyword sends an informational logging message to the console about the packet that matches the entry; the `log-input` keyword includes the input interface in the log entry.

In this example, standard named access list `stan1` denies traffic from 10.1.1.0 0.0.0.255, allows traffic from all other sources, and includes the `log` keyword.

```
Switch(config)# ip access-list standard stan1
Switch(config-std-nacl)# deny 10.1.1.0 0.0.0.255 log
Switch(config-std-nacl)# permit any log
Switch(config-std-nacl)# exit
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip access-group stan1 in
Switch(config-if)# end
```

Switch# show logging
Sylof logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
  Console logging: level debugging, 37 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 37 messages logged
  File logging: disabled
  Trap logging: level debugging, 39 message lines logged

Log Buffer (4096 bytes):
00:00:48: NTP: authentication delay calculation problems
<output truncated>

```
00:09:34:%SEC-6-IPACCESSLOGS:list stan1 permitted 0.0.0.0 1 packet
00:09:59:%SEC-6-IPACCESSLOGS:list stan1 denied 10.1.1.15 1 packet
00:10:11:%SEC-6-IPACCESSLOGS:list stan1 permitted 0.0.0.0 1 packet
```

This example is a named extended access list `ext1` that permits ICMP packets from any source to 10.1.1.0 0.0.0.255 and denies all UDP packets.

```
Switch(config)# ip access-list extended ext1
Switch(config-ext-nacl)# permit icmp any 10.1.1.0 0.0.0.255 log
Switch(config-ext-nacl)# deny udp any any log
Switch(config-ext-nacl)# exit
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# ip access-group ext1 in
```
This is an example of a log for an extended ACL:

```
01:24:23:%SEC-6-IPACCESSLOGDP:list ext1 permitted icmp 10.1.1.15 -> 10.1.1.61 (0/0), 1 packet
01:25:14:%SEC-6-IPACCESSLOGDP:list ext1 permitted icmp 10.1.1.15 -> 10.1.1.61 (0/0), 7 packets
01:26:12:%SEC-6-IPACCESSLOGDP:list ext1 denied udp 0.0.0.0(0) -> 255.255.255.255(0), 1 packet
01:31:33:%SEC-6-IPACCESSLOGDP:list ext1 denied udp 0.0.0.0(0) -> 255.255.255.255(0), 8 packets
```

Note that all logging entries for IP ACLs start with `%SEC-6-IPACCESSLOG` with minor variations in format depending on the kind of ACL and the access entry that has been matched.

This is an example of an output message when the `log-input` keyword is entered:

```
00:04:21:%SEC-6-IPACCESSLOGDP:list inputlog permitted icmp 10.1.1.10 (Vlan1 0001.42ef.a400) -> 10.1.1.61 (0/0), 1 packet
```

A log message for the same sort of packet using the `log` keyword does not include the input interface information:

```
00:05:47:%SEC-6-IPACCESSLOGDP:list inputlog permitted icmp 10.1.1.10 -> 10.1.1.61 (0/0), 1 packet
```

### Creating Named MAC Extended ACLs

You can filter non-IPv4 traffic on a VLAN or on a Layer 2 interface by using MAC addresses and named MAC extended ACLs. The procedure is similar to that of configuring other extended named ACLs.

**Note**

You cannot apply named MAC extended ACLs to Layer 3 interfaces.

For more information about the supported non-IPv4 protocols in the `mac access-list extended` command, see the command reference for this release.

**Note**

Though visible in the command-line help strings, `appletalk` is not supported as a matching condition for the `deny` and `permit` MAC access-list configuration mode commands.

Beginning in privileged EXEC mode, follow these steps to create a named MAC extended ACL:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>mac access-list extended</td>
<td>Define an extended MAC access list using a name.</td>
</tr>
</tbody>
</table>
Creating Named MAC Extended ACLs

Chapter 33  Configuring Network Security with ACLs

Use the `no mac access-list extended name` global configuration command to delete the entire ACL. You can also delete individual ACEs from named MAC extended ACLs.

This example shows how to create and display an access list named `mac1`, denying only EtherType DECnet Phase IV traffic, but permitting all other types of traffic.

```
Switch(config)# mac access-list extended mac1
Switch(config-ext-macl)# deny any any decnet-iv
Switch(config-ext-macl)# permit any any
Switch(config-ext-macl)# end
Switch # show access-lists
Extended MAC access list mac1
  10 deny   any any decnet-iv
  20 permit any any
```

Applying a MAC ACL to a Layer 2 Interface

After you create a MAC ACL, you can apply it to a Layer 2 interface to filter non-IPv4 traffic coming in that interface. When you apply the MAC ACL, consider these guidelines:

- If you apply an ACL to a Layer 2 interface that is a member of a VLAN, the Layer 2 (port) ACL takes precedence over an input Layer 3 ACL applied to the VLAN interface or a VLAN map applied to the VLAN. Incoming packets received on the Layer 2 port are always filtered by the port ACL.
- You can apply no more than one IP access list and one MAC access list to the same Layer 2 interface. The IP access list filters only IPv4 packets, and the MAC access list filters non-IPv4 packets.
A Layer 2 interface can have only one MAC access list. If you apply a MAC access list to a Layer 2 interface that has a MAC ACL configured, the new ACL replaces the previously configured one.

Beginning in privileged EXEC mode, follow these steps to apply a MAC access list to control access to a Layer 2 interface:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>interface interface-id</td>
<td>Identify a specific interface, and enter interface configuration mode. The interface must be a physical Layer 2 interface (port ACL).</td>
</tr>
<tr>
<td></td>
<td>mac access-group {name} {in}</td>
<td>Control access to the specified interface by using the MAC access list.</td>
</tr>
<tr>
<td></td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>show mac access-group [interface interface-id]</td>
<td>Display the MAC access list applied to the interface or all Layer 2 interfaces.</td>
</tr>
<tr>
<td></td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To remove the specified access group, use the no mac access-group {name} interface configuration command.

This example shows how to apply MAC access list mac1 on an interface to filter packets entering the interface:

Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# mac access-group mac1 in

**Note** The mac access-group interface configuration command is only valid when applied to a physical Layer 2 interface. You cannot use the command on EtherChannel port channels.

After receiving a packet, the switch checks it against the inbound ACL. If the ACL permits it, the switch continues to process the packet. If the ACL rejects the packet, the switch discards it. When you apply an undefined ACL to an interface, the switch acts as if the ACL has not been applied and permits all packets. Remember this behavior if you use undefined ACLs for network security.

### Configuring VLAN Maps

This section describes how to configure VLAN maps, which is the only way to control filtering within a VLAN. VLAN maps have no direction. To filter traffic in a specific direction by using a VLAN map, you need to include an ACL with specific source or destination addresses. If there is a match clause for that type of packet (IP or MAC) in the VLAN map, the default action is to drop the packet if the packet does not match any of the entries within the map. If there is no match clause for that type of packet, the default is to forward the packet.

**Note** For complete syntax and usage information for the commands used in this section, see the command reference for this release.
To create a VLAN map and apply it to one or more VLANs, perform these steps:

Step 1  Create the standard or extended IP ACLs or named MAC extended ACLs that you want to apply to the VLAN. See the “Creating Standard and Extended IP ACLs” section on page 33-7 and the “Creating a VLAN Map” section on page 33-31.

Step 2  Enter the `vlan access-map` global configuration command to create a VLAN ACL map entry.

Step 3  In access map configuration mode, optionally enter an `action — forward` (the default) or `drop` — and enter the `match` command to specify an IPv4 packet or a non-IPv4 packet (with only a known MAC address) and to match the packet against one or more ACLs (standard or extended).

Note  If the VLAN map is configured with a match clause for a type of packet (IP or MAC) and the map action is drop, all packets that match the type are dropped. If the VLAN map has no match clause, and the configured action is drop, then all IP and Layer 2 packets are dropped.

Step 4  Use the `vlan filter` global configuration command to apply a VLAN map to one or more VLANs.

This section contains these topics:

- VLAN Map Configuration Guidelines, page 33-30
- Creating a VLAN Map, page 33-31
- Applying a VLAN Map to a VLAN, page 33-34
- Using VLAN Maps in Your Network, page 33-34

**VLAN Map Configuration Guidelines**

Follow these guidelines when configuring VLAN maps:

- If there is no ACL configured to deny traffic on an interface and no VLAN map is configured, all traffic is permitted.
- Each VLAN map consists of a series of entries. The order of entries in an VLAN map is important. A packet that comes into the switch is tested against the first entry in the VLAN map. If it matches, the action specified for that part of the VLAN map is taken. If there is no match, the packet is tested against the next entry in the map.
- If the VLAN map has at least one match clause for the type of packet (IP or MAC) and the packet does not match any of these match clauses, the default is to drop the packet. If there is no match clause for that type of packet in the VLAN map, the default is to forward the packet.
- The system might take longer to boot if you have configured a very large number of ACLs.
- Logging is not supported for VLAN maps.
- If VLAN map configuration cannot be applied in hardware, all packets in that VLAN must be bridged and routed by software.
- When a switch has an IP access list or MAC access list applied to a Layer 2 interface, and you apply a VLAN map to a VLAN that the port belongs to, the port ACL takes precedence over the VLAN map.
- See the “Using VLAN Maps in Your Network” section on page 33-34 for configuration examples.
• For information about using both router ACLs and VLAN maps, see the “Guidelines” section on page 33-37.

Creating a VLAN Map

Each VLAN map consists of an ordered series of entries. Beginning in privileged EXEC mode, follow these steps to create, add to, or delete a VLAN map entry:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 vlan access-map name [number]</td>
<td>Create a VLAN map, and give it a name and (optionally) a number. The number is the sequence number of the entry within the map. When you create VLAN maps with the same name, numbers are assigned sequentially in increments of 10. When modifying or deleting maps, you can enter the number of the map entry that you want to modify or delete. Entering this command changes to access-map configuration mode.</td>
</tr>
<tr>
<td>Step 3 action {drop</td>
<td>forward}</td>
</tr>
<tr>
<td>Step 4 match [ip</td>
<td>mac] address {name</td>
</tr>
<tr>
<td>Step 5 end</td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td>Step 6 show running-config</td>
<td>Display the access list configuration.</td>
</tr>
<tr>
<td>Step 7 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Use the no vlan access-map name global configuration command to delete a map.

Use the no vlan access-map name number global configuration command to delete a single sequence entry from within the map.

Use the no action access-map configuration command to enforce the default action, which is to forward.

VLAN maps do not use the specific permit or deny keywords. To deny a packet by using VLAN maps, create an ACL that would match the packet, and set the action to drop. A permit in the ACL counts as a match. A deny in the ACL means no match.
Examples of ACLs and VLAN Maps

These examples show how to create ACLs and VLAN maps that for specific purposes.

Example 1

This example shows how to create an ACL and a VLAN map to deny a packet. In the first map, any packets that match the ip1 ACL (TCP packets) would be dropped. You first create the ip1 ACL to permit any TCP packet and no other packets. Because there is a match clause for IP packets in the VLAN map, the default action is to drop any IP packet that does not match any of the match clauses.

```
Switch(config)# ip access-list extended ip1
Switch(config-ext-nacl)# permit tcp any any
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map map_1 10
Switch(config-access-map)# match ip address ip1
Switch(config-access-map)# action drop
```

This example shows how to create a VLAN map to permit a packet. ACL ip2 permits UDP packets and any packets that match the ip2 ACL are forwarded. In this map, any IP packets that did not match any of the previous ACLs (that is, packets that are not TCP packets or UDP packets) would get dropped.

```
Switch(config)# ip access-list extended ip2
Switch(config-ext-nacl)# permit udp any any
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map map_1 20
Switch(config-access-map)# match ip address ip2
Switch(config-access-map)# action forward
```

Example 2

In this example, the VLAN map has a default action of drop for IP packets and a default action of forward for MAC packets. Used with standard ACL 101 and extended named access lists igmp-match and tcp-match, the map will have the following results:

- Forward all UDP packets
- Drop all IGMP packets
- Forward all TCP packets
- Drop all other IP packets
- Forward all non-IPv4 packets

```
Switch(config)# access-list 101 permit udp any any
Switch(config)# ip access-list extended igmp-match
Switch(config-ext-nacl)# permit igmp any any
Switch(config)# ip access-list extended tcp-match
Switch(config-ext-nacl)# permit tcp any any
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map drop-ip-default 10
Switch(config-access-map)# match ip address 101
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
Switch(config)# vlan access-map drop-ip-default 20
Switch(config-access-map)# match ip address igmp-match
Switch(config-access-map)# action drop
Switch(config-access-map)# exit
Switch(config)# vlan access-map drop-ip-default 30
Switch(config-access-map)# match ip address tcp-match
Switch(config-access-map)# action forward
```
Example 3

In this example, the VLAN map has a default action of drop for MAC packets and a default action of forward for IP packets. Used with MAC extended access lists **good-hosts** and **good-protocols**, the map will have the following results:

- Forward MAC packets from hosts 0000.0c00.0111 and 0000.0c00.0211
- Forward MAC packets with decnet-iv or vines-ip protocols
- Drop all other non-IPv4 packets
- Forward all IP packets

```shell
Switch(config)# mac access-list extended good-hosts
Switch(config-ext-macl)# permit host 0000.0c00.0111 any
Switch(config-ext-macl)# permit host 0000.0c00.0211 any
Switch(config-ext-nacl)# exit
Switch(config)# mac access-list extended good-protocols
Switch(config-ext-macl)# permit any any decnet-ip
Switch(config-ext-macl)# permit any any vines-ip
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map drop-mac-default 10
Switch(config-access-map)# match mac address good-hosts
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
Switch(config)# vlan access-map drop-mac-default 20
Switch(config-access-map)# match mac address good-protocols
Switch(config-access-map)# action forward
```

Example 4

In this example, the VLAN map has a default action of drop for all packets (IPv4 and non-IPv4). Used with access lists **tcp-match** and **good-hosts** from Examples 2 and 3, the map will have the following results:

- Forward all TCP packets
- Forward MAC packets from hosts 0000.0c00.0111 and 0000.0c00.0211
- Drop all other IP packets
- Drop all other MAC packets

```shell
Switch(config)# vlan access-map drop-all-default 10
Switch(config-access-map)# match ip address tcp-match
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
Switch(config)# vlan access-map drop-all-default 20
Switch(config-access-map)# match mac address good-hosts
Switch(config-access-map)# action forward
```
Applying a VLAN Map to a VLAN

Beginning in privileged EXEC mode, follow these steps to apply a VLAN map to one or more VLANs:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2: vlan filter mapname vlan-list list</td>
<td>Apply the VLAN map to one or more VLAN IDs. The list can be a single VLAN ID (22), a consecutive list (10-22), or a string of VLAN IDs (12, 22, 30). Spaces around the comma and hyphen are optional.</td>
</tr>
<tr>
<td>Step 3: show running-config</td>
<td>Display the access list configuration.</td>
</tr>
<tr>
<td>Step 4: copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To remove the VLAN map, use the `no vlan filter mapname vlan-list list` global configuration command.

This example shows how to apply VLAN map 1 to VLANs 20 through 22:

```
Switch(config)# vlan filter map 1 vlan-list 20-22
```

Using VLAN Maps in Your Network

This section describes some typical uses for VLAN maps and includes these topics:

- Wiring Closet Configuration, page 33-34
- Denying Access to a Server on Another VLAN, page 33-35

Wiring Closet Configuration

In a wiring closet configuration, routing might not be enabled on the switch. In this configuration, the switch can still support a VLAN map and a QoS classification ACL. In Figure 33-4, assume that Host X and Host Y are in different VLANs and are connected to wiring closet switches A and C. Traffic from Host X to Host Y is eventually being routed by Switch B, which has routing enabled. Traffic from Host X to Host Y can be access-controlled at the traffic entry point, Switch A.
If you do not want HTTP traffic switched from Host X to Host Y, you can configure a VLAN map on
Switch A to drop all HTTP traffic from Host X (IP address 10.1.1.32) to Host Y (IP address 10.1.1.34)

First, define the IP access list http that permits (matches) any TCP traffic on the HTTP port.

```
Switch(config)# ip access-list extended http
Switch(config-ext-nacl)# permit tcp host 10.1.1.32 host 10.1.1.34 eq www
Switch(config-ext-nacl)# exit
```

Next, create VLAN access map map2 so that traffic that matches the http access list is dropped and all
other IP traffic is forwarded.

```
Switch(config)# vlan access-map map2 10
Switch(config-access-map)# match ip address http
Switch(config-access-map)# action drop
Switch(config-access-map)# exit
Switch(config)# ip access-list extended match_all
Switch(config-ext-nacl)# permit ip any any
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map map2 20
Switch(config-access-map)# match ip address match_all
Switch(config-access-map)# action forward
```

Then, apply VLAN access map map2 to VLAN 1.

```
Switch(config)# vlan filter map2 vlan 1
```

### Denying Access to a Server on Another VLAN

You can restrict access to a server on another VLAN. For example, server 10.1.1.100 in VLAN 10 needs
to have access denied to these hosts (see Figure 33-5).

- Hosts in subnet 10.1.2.0/8 in VLAN 20 should not have access.
- Hosts 10.1.1.4 and 10.1.1.8 in VLAN 10 should not have access.
This example shows how to deny access to a server on another VLAN by creating the VLAN map SERVER1 that denies access to hosts in subnet 10.1.2.0/8, host 10.1.1.4, and host 10.1.1.8 and permits other IP traffic. The final step is to apply the map SERVER1 to VLAN 10.

**Step 1** Define the IP ACL that will match the correct packets.

```
Switch(config)# ip access-list extended SERVER1_ACL
Switch(config-ext-nacl)# permit ip 10.1.2.0 0.0.0.255 host 10.1.1.100
Switch(config-ext-nacl)# permit ip host 10.1.1.4 host 10.1.1.100
Switch(config-ext-nacl)# permit ip host 10.1.1.8 host 10.1.1.100
Switch(config-ext-nacl)# exit
```

**Step 2** Define a VLAN map using this ACL that will drop IP packets that match SERVER1_ACL and forward IP packets that do not match the ACL.

```
Switch(config)# vlan access-map SERVER1_MAP
Switch(config-access-map)# match ip address SERVER1_ACL
Switch(config-access-map)# action drop
Switch(config)# vlan access-map SERVER1_MAP 20
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
```

**Step 3** Apply the VLAN map to VLAN 10.

```
Switch(config)# vlan filter SERVER1_MAP vlan-list 10.
```

---

**Using VLAN Maps with Router ACLs**

To access control both bridged and routed traffic, you can use VLAN maps only or a combination of router ACLs and VLAN maps. You can define router ACLs on both input and output routed VLAN interfaces, and you can define a VLAN map to access control the bridged traffic.

If a packet flow matches a VLAN-map deny clause in the ACL, regardless of the router ACL configuration, the packet flow is denied.
When you use router ACLs with VLAN maps, packets that require logging on the router ACLs are not logged if they are denied by a VLAN map.

If the VLAN map has a match clause for the type of packet (IP or MAC) and the packet does not match the type, the default is to drop the packet. If there is no match clause in the VLAN map, and no action specified, the packet is forwarded if it does not match any VLAN map entry.

This section includes this information about using VLAN maps with router ACLs:
- Guidelines, page 33-37
- Examples of Router ACLs and VLAN Maps Applied to VLANs, page 33-38

**Guidelines**

These guidelines are for configurations where you need to have a router ACL and a VLAN map on the same VLAN. These guidelines do not apply to configurations where you are mapping router ACLs and VLAN maps on different VLANs.

The switch hardware provides one lookup for security ACLs for each direction (input and output); therefore, you must merge a router ACL and a VLAN map when they are configured on the same VLAN. Merging the router ACL with the VLAN map might significantly increase the number of ACEs.

If you must configure a router ACL and a VLAN map on the same VLAN, use these guidelines for both router ACL and VLAN map configuration:
- You can configure only one VLAN map and one router ACL in each direction (input/output) on a VLAN interface.
- Whenever possible, try to write the ACL with all entries having a single action except for the final, default action of the other type. That is, write the ACL using one of these two forms:
  ```
  permit...
  permit...
  permit...
  deny ip any any
  or
  deny...
  deny...
  deny...
  permit ip any any
  ```
- To define multiple actions in an ACL (permit, deny), group each action type together to reduce the number of entries.
- Avoid including Layer 4 information in an ACL; adding this information complicates the merging process. The best merge results are obtained if the ACLs are filtered based on IP addresses (source and destination) and not on the full flow (source IP address, destination IP address, protocol, and protocol ports). It is also helpful to use *don’t care* bits in the IP address, whenever possible.

If you need to specify the full-flow mode and the ACL contains both IP ACEs and TCP/UDP/ICMP ACEs with Layer 4 information, put the Layer 4 ACEs at the end of the list. This gives priority to the filtering of traffic based on IP addresses.
Examples of Router ACLs and VLAN Maps Applied to VLANs

This section gives examples of applying router ACLs and VLAN maps to a VLAN for switched, bridged, routed, and multicast packets. Although the following illustrations show packets being forwarded to their destination, each time the packet’s path crosses a line indicating a VLAN map or an ACL, it is also possible that the packet might be dropped, rather than forwarded.

ACLs and Switched Packets

Figure 33-6 shows how an ACL is applied on packets that are switched within a VLAN. Packets switched within the VLAN without being routed or forwarded by fallback bridging are only subject to the VLAN map of the input VLAN.

ACLs and Bridged Packets

Figure 33-7 shows how an ACL is applied on fallback-bridged packets. For bridged packets, only Layer 2 ACLs are applied to the input VLAN. Only non-IPv4, non-ARP packets can be fallback-bridged.
Figure 33-7 Applying ACLs on Bridged Packets

Figure 33-8 Applying ACLs on Routed Packets

**ACLs and Routed Packets**

Figure 33-8 shows how ACLs are applied on routed packets. For routed packets, the ACLs are applied in this order:

1. VLAN map for input VLAN
2. Input router ACL
3. Output router ACL
4. VLAN map for output VLAN
ACLs and Multicast Packets

Figure 33-9 shows how ACLs are applied on packets that are replicated for IP multicasting. A multicast packet being routed has two different kinds of filters applied: one for destinations that are other ports in the input VLAN and another for each of the destinations that are in other VLANs to which the packet has been routed. The packet might be routed to more than one output VLAN, in which case a different router output ACL and VLAN map would apply for each destination VLAN.

The final result is that the packet might be permitted in some of the output VLANs and not in others. A copy of the packet is forwarded to those destinations where it is permitted. However, if the input VLAN map (VLAN 10 map in Figure 33-9) drops the packet, no destination receives a copy of the packet.

Displaying ACL Configuration

You can display the ACLs that are configured on the switch, and you can display the ACLs that have been applied to interfaces and VLANs.

When you use the `ip access-group` interface configuration command to apply ACLs to a Layer 2 or 3 interface, you can display the access groups on the interface. You can also display the MAC ACLs applied to a Layer 2 interface. You can use the privileged EXEC commands as described in Table 33-2 to display this information.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show access-lists</code></td>
<td>Display the contents of one or all current IP and MAC address access lists or a specific access list (numbered or named).</td>
</tr>
<tr>
<td><code>show ip access-lists</code></td>
<td>Display the contents of all current IP access lists or a specific IP access list (numbered or named).</td>
</tr>
</tbody>
</table>
Chapter 33 Configuring Network Security with ACLs

Displaying ACL Configuration

You can also display information about VLAN access maps or VLAN filters. Use the privileged EXEC commands in Table 33-3 to display VLAN map information.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip interface interface-id</td>
<td>Display detailed configuration and status of an interface. If IP is enabled on the interface and ACLs have been applied by using the <code>ip access-group</code> interface configuration command, the access groups are included in the display.</td>
</tr>
<tr>
<td>show running-config [interface interface-id]</td>
<td>Displays the contents of the configuration file for the switch or the specified interface, including all configured MAC and IP access lists and which access groups are applied to an interface.</td>
</tr>
<tr>
<td>show mac access-group [interface interface-id]</td>
<td>Displays MAC access lists applied to all Layer 2 interfaces or the specified Layer 2 interface.</td>
</tr>
</tbody>
</table>

Table 33-3 Commands for Displaying VLAN Map Information

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show vlan access-map [mapname]</td>
<td>Show information about all VLAN access-maps or the specified access map.</td>
</tr>
<tr>
<td>show vlan filter [access-map name</td>
<td>vlan vlan-id]</td>
</tr>
</tbody>
</table>
Configuring QoS

This chapter describes how to use different methods to configure quality of service (QoS) on the Catalyst 3750 Metro switch. With QoS, you can provide preferential treatment to certain types of traffic at the expense of others. Without QoS, the switch offers best-effort service to each packet, regardless of the packet contents or size. It sends the packets without any assurance of reliability, delay bounds, or throughput.

You can use auto-QoS to identify ports connected to Cisco IP Phones and to devices running the Cisco SoftPhone application. You also use the commands to identify ports that receive trusted voice over IP (VoIP) traffic.

You can use standard QoS to classify, police, mark, queue, and schedule inbound traffic on any port as well as queue and schedule outbound traffic. On ingress, standard QoS offers classification based on the class of service (CoS), Differentiated Services Code Point (DSCP), or IP precedence value in the inbound packet. You can perform the classification based on Layer 2 MAC, IP-standard, or IP-extended access control lists (ACLs). Standard QoS also offers nonhierarchical single-level policy maps on physical ports and hierarchical dual-level policy maps on switch virtual interfaces (SVIs). Drop policy actions are passing through the packet without modification, marking down the assigned DSCP in the packet, or dropping the packet. Standard QoS performs ingress queueing based on the weighted tail drop (WTD) algorithm and ingress scheduling based on shaped round robin (SRR). On egress, standard QoS offers queueing based on WTD and scheduling based on SRR shared or shaped weights. An egress priority queue is also offered.

Note: In the Catalyst 3750, 3560, and 2970 switch software documentation, single-level policy maps are referred to as nonhierarchical policy maps. Dual-level policy maps are referred to as hierarchical policy maps with two levels.

You can use hierarchical QoS to classify, police, mark, queue, and schedule inbound or outbound traffic on an enhanced-services (ES) port or an EtherChannel of ES ports. Hierarchical QoS offers classification based on the CoS, DSCP, IP precedence, or the multiprotocol label switching (MPLS) experimental (EXP) bits in the packet. You also can classify a packet based on its VLAN. Hierarchical QoS offers two-rate traffic policing. Drop policy actions are passing the packet through without modification; marking down the CoS, DSCP, IP precedence, or the MPLS EXP bits in the packet; or dropping the packet. Hierarchical QoS performs queueing based on tail drop or Weighted Random Early Detection (WRED). The queue scheduling management feature is class-based weighted fair queueing (CBWFQ), and the scheduling congestion-management feature is low-latency queueing (LLQ). You can use traffic shaping to decrease the burstiness of traffic.

For information about MPLS, Ethernet over MPLS (EoMPLS), and QoS, see the “Configuring MPLS and EoMPLS QoS” section on page 44-51.
QoS Overview

Typically, networks operate on a best-effort delivery basis, which means that all traffic has equal priority and an equal chance of being delivered in a timely manner. When congestion occurs, all traffic has an equal chance of being dropped.

When you configure the QoS feature, you can select specific network traffic, prioritize it according to its relative importance, and use congestion-management and congestion-avoidance techniques to provide preferential treatment. Implementing QoS in your network makes network performance more predictable and bandwidth utilization more effective.

The QoS implementation is based on the Differentiated Services (Diff-Serv) architecture, an emerging standard from the Internet Engineering Task Force (IETF). This architecture specifies that each packet is classified upon entry into the network.

The classification is carried in the IP packet header, using 6 bits from the deprecated IP type of service (ToS) field to carry the classification (class) information. Classification also can be carried in the Layer 2 frame. These special bits in the Layer 2 frame or in the Layer 3 packet are described here and shown in Figure 34-1:

- Prioritization bits in Layer 2 frames:
  - Layer 2 Inter-Switch Link (ISL) frame headers have a 1-byte User field that carries an IEEE 802.1p CoS value in the three least-significant bits. On ports configured as Layer 2 ISL trunks, all traffic is in ISL frames.
  - Layer 2 802.1Q frame headers have a 2-byte Tag Control Information field that carries the CoS value in the three most-significant bits, which are called the User Priority bits. On ports configured as Layer 2 802.1Q trunks, all traffic is in IEEE 802.1Q frames except for traffic in the native VLAN. Other frame types cannot carry Layer 2 CoS values.
Layer 2 CoS values range from 0 for low priority to 7 for high priority.

- Prioritization bits in Layer 3 packets:
  Layer 3 IP packets can carry either an IP precedence value or a DSCP value. QoS supports the use of either value because DSCP values are backward-compatible with IP precedence values.
  - IP precedence values range from 0 to 7.
  - DSCP values range from 0 to 63.
- Cisco IOS Release 12.2(52)SE and later supports IPv6 port-based trust with the dual IPv4 and IPv6 Switch Database Management (SDM) templates. You must reload the switch with the dual IPv4 and IPv6 templates for switches running IPv6. For more information, see Chapter 6, “Configuring SDM Templates.”

**Figure 34-1  QoS Classification Layers in Frames and Packets**

Encapsulated Packet

Layer 2 ISL Frame

Layer 2 802.1Q and 802.1p Frame

Layer 3 IPv4 Packet

Layer 3 IPv6 Packet

**Note**

Layer 3 IPv6 packets are treated as non-IP packets and are bridged by the switch.

All switches and routers that access the Internet rely on the class information to provide the same forwarding treatment to packets with the same class information and different treatment to packets with different class information. The class information in the packet can be assigned by end hosts or by switches or routers along the way, based on a configured policy, detailed examination of the packet, or both. Detailed examination of the packet is expected to happen closer to the edge of the network so that the core switches and routers are not overloaded with this task.
Switches and routers along the path can use the class information to limit the amount of resources allocated per traffic class. The behavior of an individual device when handling traffic in the DiffServ architecture is called per-hop behavior. If all devices along a path provide a consistent per-hop behavior, you can construct an end-to-end QoS solution.

Implementing QoS in your network can be a simple or complex task and depends on the QoS features offered by your internetworking devices, the traffic types and patterns in your network, and the degree of control that you need over inbound and outbound traffic.

**Basic QoS Model**

Figure 34-2 shows the basic QoS model for traffic on all ports, including ES ports.
To implement QoS, the switch must distinguish (classify) packets or flows from one another, assign a label to indicate the given quality of service as the packets move through the switch, make the packets comply with the configured resource usage limits (police and mark), and provide different treatment (queue and schedule) in all situations where resource contention exists. The switch also needs to ensure that the traffic it sends meets a specific traffic profile (shape).
These are the standard actions when traffic is received on any port:

- Classification is the process of generating a distinct path for a packet by associating it with a QoS label. The switch maps the CoS or DSCP in the packet to a QoS label to distinguish one kind of traffic from another. The QoS label that is generated identifies all future QoS actions to be performed on this packet. For more information, see the “Ingress Classification” section on page 34-9.

- Policing decides whether a packet is in or out of profile by comparing the rate of the inbound traffic to the configured policer. The policer limits the bandwidth consumed by a flow of traffic. The result is passed to the marker. For more information, see the “Ingress Policing and Marking” section on page 34-13.

- Marking evaluates the policer configuration information for the action to take when a packet is out of profile. Marking actions are to pass through a packet without modification, to mark down the QoS label in the packet, or to drop the packet. For more information, see the “Ingress Policing and Marking” section on page 34-13.

- Queueing evaluates the QoS label and the corresponding DSCP or CoS value to select into which of the two ingress queues to place a packet. Queueing is enhanced with the WTD algorithm, a congestion-avoidance mechanism. If the threshold is exceeded, the packet is dropped. For more information, see the “Queueing and Scheduling Overview” section on page 34-17.

- Scheduling services the queues based on their configured (SRR) weights. One of the ingress queues is the priority queue, and SRR services it for its configured share before servicing the other queue. For more information, see the “SRR Shaping and Sharing” section on page 34-19.

These are the standard actions when traffic is received on or sent to a standard port:

- Queueing evaluates the QoS label and the corresponding DSCP or CoS value to select into which queue-set (a set of four queues per port) to place a packet. Because congestion can occur when multiple ingress ports simultaneously send data to an egress port, WTD is used to differentiate traffic classes and to subject the packets to different thresholds based on the QoS label. If the threshold is exceeded, the packet is dropped. For more information, see the “Queueing and Scheduling Overview” section on page 34-17.

- Scheduling services the four egress queues based on their configured SRR shared or shaped weights. One of the queues (queue 1) can be the priority queue. Before servicing the other queues, SRR services the priority queue until it is empty.

These are the additional actions when traffic is received on or sent to an ES port:

- Classification is the process of generating a distinct path for a packet by matching the CoS, DSCP, IP precedence, by matching the MPLS EXP bits in the header, or by matching a packet based on the inner and the outer VLAN IDs or CoS values. The hierarchical configuration controls the number of class-level, VLAN-level, and physical-interface-level queues to create. For information, see the “Understanding Hierarchical QoS” section on page 34-30 and the “Hierarchical Levels” section on page 34-30. For classification information, see the “Hierarchical Classification Based on Traffic Classes and Traffic Policies” section on page 34-33.

- Policing decides whether a packet is in or out of profile by comparing the rate of the inbound or the outbound traffic to the configured policer. The policer limits the bandwidth consumed by a flow of traffic. The result is passed to the marker. For more information, see the “Hierarchical Policies and Marking” section on page 34-34.

- Marking evaluates the policer and configuration information for the action to be taken when a packet is out of profile and resolves what to do with the packet (pass it through without modification, mark down the QoS label, or drop). For more information, see the “Hierarchical Policies and Marking” section on page 34-34.
Queueing is accomplished through a hierarchical queueing framework, in which the switch assigns each packet to a queue based on the packet class, VLAN, and physical interface. Tail drop or WRED can be configured per queue as the congestion-avoidance mechanism. With tail drop, packets are queued until the maximum threshold is exceeded, and then all the packets are dropped. WRED reduces the chances of tail drop by selectively dropping packets when the port begins to show signs of congestion. For more information, see the “Queueing and Scheduling of Hierarchical Queues” section on page 34-37.

Scheduling is accomplished through Class-based weighted fair queueing (CBWFQ) or LLQ. CBWFQ provides guaranteed bandwidth to a particular traffic class while still fairly serving all other traffic in the network. LLQ is another scheduling mechanism, which ensures that delay-sensitive traffic is queued and sent before the traffic in other queues. Scheduling services the queues through average-rate shaping. For more information, see the “Queueing and Scheduling of Hierarchical Queues” section on page 34-37.

Supported Policy Maps

Different types of policy-map formats are supported on different interface types. These types of policy-map formats are supported:

- Single-level (nonhierarchical) policy-map: You can define actions only at the class level of the policy-map.
- Up to two-level hierarchical policy-map: You can define actions in one or two levels in this order: physical level, VLAN level, and class level. These policies are supported only on SVIs and act against all traffic received on an SVI.
- Up to three-level hierarchical policy-map: You can define actions in up to three levels with the levels defined in this order: physical level, VLAN level, and class level. These policies are supported only on ES ports and ES EtherChannels.

**Note**

Note: A two-level policy on an SVI is different than a hierarchical policy with two levels on ES ports.

Table 34-1 shows the types of policy maps supported on different interfaces.

**Table 34-1** Policy Maps Supported on Different Interface Types

<table>
<thead>
<tr>
<th>Interface type</th>
<th>Single Level</th>
<th>Dual Level (Class/Physical)</th>
<th>Hierarchical (Up to 3 levels)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Input</td>
<td>Output</td>
<td>Input</td>
</tr>
<tr>
<td>Standard port</td>
<td>Yes¹</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Enhanced services port</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Enhanced services EtherChannel</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>SVI</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

1. Yes = supported. No = not supported.

If you add an action to an unsupported policy-map format or interface, you cannot attach the service policy to the interface.

Note that different software releases also have different levels of support for policy maps:
**Basic QoS Model**

Software releases earlier than Cisco IOS Release 12.2(25)EY support:
- Nonhierarchical single-level input policy maps on standard and ES physical ports.
- Nonhierarchical single-level output policy maps on ES physical ports.
- Hierarchical (up to three-level) output policy maps on ES physical ports.

Cisco IOS Release 12.2(25)EY or later also supports:
- Hierarchical (up to three-level) input policy maps on ES physical ports
- Up to two-level hierarchical input policy maps on SVIs

Cisco IOS Release 12.2(35)SE or later also supports:
- Nonhierarchical single-level output policy maps on EtherChannels consisting of ES ports.
- Hierarchical (up to three-level) input and output policy maps on EtherChannels made of ES ports.

You can configure common hierarchical policies on ES ports and also ensure EtherChannel redundancy and load balancing.

---

**Supported Policing Configurations**

Different interface types and policy formats support different types of policing configurations.

The switch supports various forms of input policing, based on whether the input policy maps are attached to standard ports, SVIs, ES ports, or EtherChannels made of ES ports (Cisco IOS Release 12.2(35)SE or later):

- Nonhierarchical single-level input policy maps on standard and ES ports support only one-rate, two-color individual and aggregate policers, but not two-rate, three-color policers. If you need to use one of the hierarchical options without an actual hierarchy, you can create a false hierarchy (using only class-default). For more details about nonhierarchical policing, see the “Nonhierarchical Single-Level Policing” section on page 34-13.

- Hierarchical input policy maps attached to SVIs can have actions in up to two levels and support only one-rate, two-color individual policers. They do not support two-rate, three-color policers or aggregate policers. You configure the policer only at the physical level of the hierarchy. For more information about this policing configuration, see the “Hierarchical Dual-Level Policing on SVIs” section on page 34-15.

- Hierarchical input policy maps attached to ES ports (or, beginning with Cisco IOS Release 12.2(35)SE, EtherChannels consisting of ES ports) can have actions defined in up to three levels and support one-rate, two-color and two-rate, three-color individual policers with configurable actions for all colors. You can configure the policer at any one level of the hierarchy. These policy maps do not support aggregate policers. For more information on hierarchical policy maps, see the “Hierarchical Policies and Marking” section on page 34-34. For a list of differences between hierarchical policy maps on ES ports and EtherChannels, see the “Hierarchical QoS on EtherChannels” section on page 34-40.

Output policing is supported only on ES ports or EtherChannels made of ES ports (Cisco IOS Release 12.2(35)SE or later). Policing is supported in nonhierarchical and up to three-level hierarchical output policy maps. Policing in up to three-level hierarchical policies is described in the “Hierarchical Policies and Marking” section on page 34-34.
Understanding Standard QoS

Standard QoS involves standard ingress policies to classify, police, and mark traffic received on any port. Ingress queues prevent congestion by storing packets before forwarding them into the switch fabric. Egress queue-sets prevent congestion when multiple ingress ports simultaneously send packets to a port. You configure the ingress queues and the egress queue-sets for queueing and scheduling activities.

This section includes these topics:

- Ingress Classification, page 34-9
- Ingress Policing and Marking, page 34-13
- Mapping Tables, page 34-17
- Queueing and Scheduling Overview, page 34-17

Ingress Classification

Ingress classification distinguishes one kind of traffic from another by examining the fields in the packet upon receipt. Classification is enabled only if QoS is globally enabled on the switch. By default, QoS is globally disabled, so no classification occurs.

During ingress classification, the switch performs a lookup and assigns a QoS label to the packet. The QoS label identifies all QoS actions to be performed on the packet and from which queue the packet is sent.

The QoS label is based on the DSCP or the CoS value in the packet and determines the queueing and scheduling actions to perform on the packet. The label is mapped according to the trust setting and the packet type as shown in Figure 34-3 on page 34-11.

You specify which fields in the frame or the packet that you want to use to classify inbound traffic. For non-IP traffic, you have these ingress classification options, as shown in Figure 34-3:

- Trust the CoS value in the inbound frame (configure the port to trust CoS). Then use the configurable CoS-to-DSCP map to generate a DSCP value for the packet. Layer 2 ISL frame headers carry the CoS value in the three least-significant bits of the 1-byte User field. Layer 2 IEEE 802.1Q frame headers carry the CoS value in the three most-significant bits of the Tag Control Information field. CoS values range from 0 for low priority to 7 for high priority.

- Trust the DSCP or trust IP precedence value in the inbound frame. These configurations are meaningless for non-IP traffic. If you configure a port with either of these options and non-IP traffic is received, the switch assigns a CoS value and generates an internal DSCP value from the CoS-to-DSCP map. The switch uses the internal DSCP value to generate a CoS value representing the priority of the traffic.

- Perform the classification based on a configured Layer 2 MAC ACL, which can examine the MAC source address, the MAC destination address, and other fields. If no ACL is configured, the packet is assigned 0 for the DSCP and CoS values, which means best-effort traffic. Otherwise, the policy-map action specifies a DSCP or a CoS value to assign to the inbound frame.
For IP traffic, you have these ingress classification options, as shown in Figure 34-3:

- Trust the DSCP value in the inbound packet (configure the port to trust DSCP), and assign the same DSCP value to the packet. The IETF defines the six most-significant bits of the 1-byte ToS field as the DSCP. The priority represented by a particular DSCP value is configurable. DSCP values range from 0 to 63.

  For ports that are on the boundary between two QoS administrative domains, you can modify the DSCP to another value through the configurable DSCP-to-DSCP-mutation map.

- Trust the IP precedence value in the inbound packet (configure the port to trust IP precedence), and generate a DSCP value for the packet through the configurable IP-precedence-to-DSCP map. The IP Version 4 specification defines the three most-significant bits of the 1-byte ToS field as the IP precedence. IP precedence values range from 0 for low priority to 7 for high priority.

- Trust the CoS value (if present) in the inbound packet, and generate a DSCP value for the packet through the CoS-to-DSCP map. If the CoS value is not present, use the port CoS value.

- Perform the classification based on a configured IP standard or an extended ACL, which examines various fields in the IP header. If no ACL is configured, the packet is assigned 0 as the DSCP and CoS values, which means best-effort traffic. Otherwise, the policy-map action specifies a DSCP or a CoS value to assign to the inbound frame.

For information on the maps described in this section, see the “Mapping Tables” section on page 34-17. For configuration information on port trust states, see the “Configuring Ingress Classification by Using Port Trust States” section on page 34-56.

You can configure classification through ACLs, traffic classes, and traffic policies. For more information, see the “Ingress Classification Based on QoS ACLs” section on page 34-11 and the “Ingress Classification Based on Traffic Classes and Traffic Policies” section on page 34-12.

After ingress classification, the packet is sent to the policing, marking, and the ingress queueing and scheduling stages.
Ingress Classification Based on QoS ACLs

You can use IP standard, IP extended, or Layer 2 MAC ACLs to define a group of packets with the same characteristics \(\text{(class)}\). In the QoS context, the permit and deny actions in the access control entries (ACEs) have different meanings than with security ACLs:

- If a match with a permit action is encountered (first-match principle), the specified QoS-related action is taken.
### Understanding Standard QoS

- If a match with a deny action is encountered, the ACL being processed is omitted, and the next ACL is processed.
- If no match with a permit action is encountered and all the ACEs have been examined, no QoS processing occurs on the packet, and the switch offers best-effort service to the packet.
- If multiple ACLs are configured on a port, the lookup stops after the packet matches the first ACL with a permit action, and QoS processing begins.

**Note**

When you create an access list, remember that the end of the access list contains an implicit deny statement for everything if it did not find a match before reaching the end.

After a traffic class is defined with the ACL, you can attach a policy to it. A policy might contain multiple classes with actions specified for each one of them. A policy might include commands to classify the class as a particular aggregate (for example, assign a DSCP) or to rate-limit the class. This QoS policy is then attached to a port.

You implement IP ACLs to classify IP traffic by using the `access-list` global configuration command; you implement Layer 2 MAC ACLs to classify non-IP traffic by using the `mac access-list extended` global configuration command. For configuration information, see the “Configuring an Ingress QoS Policy” section on page 34-63.

### Ingress Classification Based on Traffic Classes and Traffic Policies

You define a traffic class to classify traffic, use a traffic policy to decide how to treat the classified traffic, and attach the ingress policy to a port to create a service policy.

You use the class map to define a specific traffic flow (or class) and to isolate it from all other traffic. The class map defines the criteria used to match against a specific traffic flow to further classify it. The criteria can include matching the access group defined by the ACL or matching a specific list of DSCP or IP precedence values. If you have more than one type of traffic that you want to classify, you can create another class map and use a different name.

You create a class map by using the `class-map` global configuration command. When you enter the `class-map` command, the switch enters the class-map configuration mode. In this mode, you define the match criterion for the traffic by using the `match` class-map configuration command. Inbound packets are compared to the match criteria configured for a class map to determine if the packet belongs to that class. If a packet matches the specified criteria, the packet is considered a member of the class and is forwarded according to the QoS specifications set in the traffic policy. If a packet fails to meet any of the matching criteria, it is classified as a member of the traffic class if one is configured.

You use the policy map to create the traffic policy, to specify the traffic class to act on, and to configure the QoS features associated with the traffic class. Actions on ingress can include trusting the received CoS, DSCP, or IP precedence values in the traffic class; setting a specific DSCP or IP precedence value in the traffic class; or specifying the traffic bandwidth limitations and the action to take when the traffic is out of profile.

You create and name a policy map by using the `policy-map` global configuration command. When you enter this command, the switch enters the policy-map configuration mode. In this mode, you use the `class` policy-map configuration command to name the traffic class associated with the traffic policy. If you specify `class` as the class name in the `class` policy-map configuration command, packets that fail to meet any of the matching criteria are classified as members of the traffic class. You can manipulate this class (for example, police it and mark it) just like any traffic class, but you cannot delete it. After you name the traffic class with the `class` command, the switch enters policy-map class configuration mode, and you can specify the actions to take on this traffic class.
An ingress policy map can include `police`, `police aggregate`, `trust`, or `set` policy-map class configuration commands. You attach the ingress policy map to a port by using the `service-policy input` interface configuration command.

In software releases earlier than Cisco IOS Release 12.2(25)EY, you can apply a nonhierarchical single-level policy map only to a physical port—in both directions of an ES port and in the input direction of a standard port. Hierarchical (up to three-level) policy maps were supported only as output policy maps on ES ports. Cisco IOS Release 12.2(25)EY or later also supports up to two-level policy maps in the input direction of an SVI and up to three-level policy maps as input policy maps on ES ports. However, a hierarchical dual-level policy map can only be applied to an SVI. The dual-level policy map contains two levels. The first level, the VLAN level, specifies the actions to be taken against a traffic flow on the SVI. The second level, the interface level, specifies the actions to be taken against the traffic on the physical ports that belong to the SVI. The interface-level actions are specified in the interface-level policy map. You can also use Cisco IOS Release 12.2(35)SE to apply single-level output policy maps and hierarchical input and output maps to EtherChannels consisting of ES ports.

For more information, see the “Ingress Policing and Marking” section on page 34-13. For configuration information, see the “Configuring an Ingress QoS Policy” section on page 34-63.

### Ingress Policing and Marking

After a packet is classified and has a DSCP-based or CoS-based QoS label assigned to it, the traffic policing and marking process can begin. Figure 34-4 on page 34-15 shows an ingress, single-rate traffic policer. Figure 34-5 on page 34-16 shows the ingress policing and marking process.

Ingress traffic policing controls the maximum rate of traffic received on a port. The policer defines the bandwidth limitations of the traffic and the action to take if the limits are exceeded. It is often configured on ports at the edge of a network to limit traffic into or out of the network. In most policing configurations, traffic that falls within the rate parameters is sent. Traffic that exceeds the parameters is considered to be *out of profile* or *nonconforming* and is dropped or sent with a different priority.

---

**Note**

All traffic, regardless of whether it is bridged or routed, is subjected to a configured policer. As a result, bridged packets might be dropped or might have their DSCP or CoS fields modified when they are policed and marked.

---

**Note**

Input hierarchical service policies are applied to a traffic stream before any other services act on that traffic. For example, an input hierarchical service policy applied to traffic could change the traffic rate from above a storm-control threshold to below the threshold, preventing storm control from acting on the traffic stream.

### Nonhierarchical Single-Level Policing

In nonhierarchical single-level policy maps on physical ports, you can create these types of ingress policers:

- Individual (single rate)

  QoS applies the bandwidth limits specified in the policer separately to each matched traffic class. You can configure a single-rate policer within a policy map by using the `police` policy-map class configuration command.
• Aggregate

QoS applies the bandwidth limits specified in an aggregate policer cumulatively to all matched traffic flows. You configure this type of policer by specifying the aggregate policer name within a policy map by using the `police aggregate` policy-map class configuration command. You specify the bandwidth limits of the policer by using the `mls qos aggregate-policer` global configuration command. In this way, the aggregate policer is shared by multiple classes of traffic within a policy map.

**Note** You can only configure only individual policers on SVIs and only with Cisco IOS Release 12.2(25)EY or later.

A single-rate traffic policer decides on a packet-by-packet basis whether the packet is in or out of profile and specifies the actions on the packet. These actions, carried out by the marker, include passing through the packet without modification, dropping the packet, or modifying (marking down) the assigned DSCP of the packet and allowing the packet to pass through. The configurable policed-DSCP map provides the packet with a new DSCP-based QoS label. For information on the policed-DSCP map, see the “Mapping Tables” section on page 34-17. Marked-down packets use the same queues as the original QoS label to prevent packets in a flow from getting out of order.

Single-level policing uses a token-bucket algorithm. As each frame is received by the switch, a token is added to the bucket. The bucket has a hole in it and leaks at a rate that you specify as the average traffic rate in bps. Each time a token is added to the bucket, the switch verifies that there is enough room in the bucket. If there is not enough room, the packet is marked as nonconforming, and the specified policer action is taken (dropped or marked down).

How quickly the bucket fills is a function of the bucket depth (burst-byte), the rate at which the tokens are removed (rate-bps), and the duration of the burst above the average rate. The size of the bucket imposes an upper limit on the burst length and limits the number of frames that can be sent back-to-back. If the burst is short, the bucket does not overflow, and no action is taken against the traffic flow. However, if a burst is long and at a higher rate, the bucket overflows, and the policing actions are taken against the frames in that burst.

You configure the bucket depth (the maximum burst that is tolerated before the bucket overflows) by using the `burst-byte` option of the `police` policy-map class configuration command or the `mls qos aggregate-policer` global configuration command. You configure how fast (the average rate) that the tokens are removed from the bucket by using the `rate-bps` option of the `police` policy-map class configuration command or the `mls qos aggregate-policer` global configuration command.

After you configure the policy map and policing actions, attach the ingress policy to a port by using the `service-policy input` interface configuration command. For configuration information, see the “Classifying, Policing, and Marking Ingress Traffic by Using Nonhierarchical Single-Level Policy Maps” section on page 34-69 and the “Classifying, Policing, and Marking Ingress Traffic by Using Aggregate Policers” section on page 34-79.

**Figure 34-4** shows the policing and marking process when these types of policy maps are configured:

• A nonhierarchical single-level policy map.
• The interface level of a hierarchical dual-level policy map attached to an SVI. The physical ports are specified in this secondary policy map.
Hierarchical Dual-Level Policing on SVIs

Before configuring a hierarchical dual-level policy map with individual policers on an SVI, you must enable VLAN-based QoS on the physical ports that belong to the SVI. Though a policy map is attached to the SVI, the individual policers only affect traffic on the physical ports specified in the secondary interface level of the dual-level policy map.

A dual-level policy map has two levels. The first level, the VLAN level, specifies the actions to be taken against a traffic flow on an SVI. The second level, the interface level, specifies the actions to be taken against the traffic on the physical ports that belong to the SVI and are specified in the interface-level policy map.

When configuring policing on an SVI, you can create and configure a hierarchical policy map with these two levels:

- VLAN level—Create this primary level by configuring class maps and classes that specify the port trust state or set a new DSCP or IP precedence value in the packet. The VLAN-level policy map applies only to the VLAN in an SVI and does not support policers.

Note The VLAN level in a dual-level policy map is different than the VLAN level in a hierarchical policy map that is applied on an ES port.
- Interface level—Create this secondary level by configuring class maps and classes that specify the individual policers on physical ports the belong to the SVI. The interface-level policy map only supports individual policers and does not support aggregate policers.

**Note**

You cannot include ES ports in interface level class-map configuration for a policy attached to an SVI. If you try to attach this type of service policy to an SVI, the command is rejected with an error message. To configure enhanced per-port, per-VLAN policing for an ES port, you can attach a hierarchical policy map to the port.

See the “Classifying, Policing, and Marking Traffic by Using Hierarchical Dual-Level Policy Maps” section on page 34-73 for an example of a dual-level policy map.

**Figure 34-5** shows the policing and marking process when hierarchical dual-level policy maps are attached to an SVI.

**Figure 34-5**  Ingress Hierarchical Dual-Level Policing and Marking Flowchart on SVIs
Mapping Tables

During QoS ingress processing, the switch represents the priority of all traffic (including non-IP traffic) with a QoS label based on the DSCP or CoS value from the classification stage:

- During ingress classification, QoS uses configurable mapping tables to derive a corresponding DSCP or CoS value from a received CoS, DSCP, or IP precedence value. These maps include the CoS-to-DSCP map and the IP-precedence-to-DSCP map. You configure these maps by using the `mls qos map cos-dscp` and the `mls qos map ip-prec-dscp` global configuration commands.

On an ingress port configured in the DSCP-trusted state, if the DSCP values are different between the QoS domains, you can apply the configurable DSCP-to-DSCP-mutation map to the port that is on the boundary between the two QoS domains. You configure this map by using the `mls qos map dscp-mutation` global configuration command.

- During ingress policing, QoS can assign another DSCP value to an IP or a non-IP packet (if the packet is out of profile and the policer specifies a marked-down value). This configurable map is called the policed-DSCP map. You configure this map by using the `mls qos map policed-dscp` global configuration command.

- Before the traffic reaches the scheduling stage, QoS stores the packet in an ingress and an egress queue according to the QoS label. The QoS label is based on the DSCP or the CoS value in the inbound packet. The QoS label selects an ingress queue and an egress queue from the queue-set through the DSCP input and output queue threshold maps or through the CoS input and output queue threshold maps. In addition to an ingress or an egress queue, the QOS label also identifies the WTD threshold value. You configure these maps by using the `mls qos srr-queue {input | output} dscp-map` and the `mls qos srr-queue {input | output} cos-map` global configuration commands.

- When marking and queueing CPU-generated traffic:
  - If you explicitly configure the output queue by entering the `mls qos srr-queue output cpu-queue` global configuration command, the CPU traffic is sent to that queue, and the threshold value applies to that queue.
  - If you do not explicitly configure the output queue for CPU-generated traffic, the cpu marking values and the dscp-map or cos-map values determine the output queue and the threshold for the CPU-generated traffic.

The CoS-to-DSCP, DSCP-to-CoS, and the IP-precedence-to-DSCP maps have values that might or might not be appropriate for your network.

The DSCP-to-DSCP-mutation map and the policed-DSCP map are null maps; they map an inbound DSCP value to the same DSCP value. The DSCP-to-DSCP-mutation map is the only map that you apply to a specific port. All other maps apply to the entire switch.

For configuration information, see the “Configuring DSCP Maps” section on page 34-80.

For information about the DSCP and CoS input queue threshold maps, see the “Queueing and Scheduling of Ingress Queues” section on page 34-20. For information about the DSCP and CoS output queue threshold maps, see the “Queueing and Scheduling of Egress Queue-Sets” section on page 34-22.

Queueing and Scheduling Overview

The switch has queues at specific points to help prevent congestion, as shown in Figure 34-6. Figure 34-6 shows the ingress and egress queues for traffic on all ports, including ES ports.
Because the total ingress bandwidth of all ports can exceed the bandwidth of the internal ring, ingress queues are located after the packet is classified, policed, and marked and before packets are forwarded into the switch fabric. Because multiple ingress ports can simultaneously send packets to an egress port and cause congestion, egress queue-sets are located after the internal ring.

Each port belongs to an egress queue-set, which defines all the characteristics of the four queues per port. The ES ports also use a hierarchical queueing model in which each packet is assigned to a hierarchical queue based on the physical interface, VLAN, or class. Traffic received from or destined for an ES port passes through the queue-set. If congestion occurs in the hierarchical queues and backs up to the queue-sets, the queue-set configuration controls how traffic is dropped.

Ingress queues use WTD for congestion management. The egress queue-sets also use WTD. For more information, see the next section.

Ingress queues support SRR in shared mode for scheduling. The egress queue-sets also support SRR in shared or shaped mode for scheduling. For more information, see the “SRR Shaping and Sharing” section on page 34-19.

For information about ingress queueing and scheduling, see the “Queueing and Scheduling of Ingress Queues” section on page 34-20. For information about egress queue-set queueing and scheduling, see the “Queueing and Scheduling of Egress Queue-Sets” section on page 34-22.

The hierarchical queues for ES ports use tail drop or WRED for congestion management. These ports also use CBWFQ or LLQ for scheduling. For more information, see the “Queueing and Scheduling of Hierarchical Queues” section on page 34-37.
Weighted Tail Drop

The ingress queues and the egress queue-sets use an enhanced version of the tail-drop congestion-avoidance mechanism called Weighted Tail Drop (WTD). WTD manages the queue lengths and provides drop precedences for different traffic classifications.

As a frame is sent to a particular queue, WTD uses the assigned QoS label of the frame to subject it to different thresholds. If the threshold is exceeded for that QoS label (the space available in the destination queue is less than the size of the frame), the switch drops the frame.

Each queue has three threshold values. The QOS label is determines which of the three threshold values is subjected to the frame. Of the three thresholds, two are configurable (explicit) and one is not (implicit).

Figure 34-7 shows an example of WTD operating on a queue whose size is 1000 frames. Three drop percentages are configured: 40, 60, and 100 percent. These percentages mean that up to 400 frames can be queued at the 40-percent threshold, up to 600 frames at the 60-percent threshold, and up to 1000 frames at the 100-percent threshold.

In this example, CoS values 6 and 7 have a greater importance than the other CoS values, and they are assigned to the 100-percent drop threshold (queue-full state). CoS values 4 and 5 are assigned to the 60-percent threshold, and CoS values 0 to 3 are assigned to the 40-percent threshold.

Suppose the queue is already filled with 600 frames, and a new frame arrives. It contains CoS values 4 and 5 and is subjected to the 60-percent threshold. If this frame is added to the queue, the threshold will be exceeded, so the switch drops it.

Figure 34-7 WTD and Queue Operation

For more information, see the “Mapping DSCP or CoS Values to an Ingress Queue and Setting WTD Thresholds” section on page 34-87, the “Allocating Buffer Space to and Setting WTD Thresholds for an Egress Queue-Set” section on page 34-91, and the “Mapping DSCP or CoS Values to an Egress Queue-Set and to a Threshold ID” section on page 34-93.

SRR Shaping and Sharing

The ingress queues and egress queue-sets are serviced by SRR, which controls the rate at which packets are sent. On the ingress queues, SRR sends packets to the internal ring. On the egress queue-sets, SRR sends packets to a standard port.

You can configure SRR on the egress queue-sets for sharing or for shaping. However, for ingress queues, sharing is the mode and is the only mode supported.

In shaped mode, the queues are guaranteed a percentage of the bandwidth, and they are rate-limited to that amount. Shaped traffic does not use more than the allocated bandwidth even if the link is idle. Shaping provides a more even flow of traffic over time and reduces the peaks and valleys of bursty traffic. With shaping, the absolute value of each weight is used to compute the bandwidth available for the queues.
In shared mode, the queues share the bandwidth among them according to the configured weights. The bandwidth is guaranteed at this level but not limited to it. For example, if a queue is empty and no longer requires a share of the link, the remaining queues can expand into the unused bandwidth and share it among them. With sharing, the ratio of the weights controls the frequency of dequeuing; the absolute values are meaningless. Shaping and sharing is configured per interface. Each interface can be uniquely configured.

For more information, see the “Allocating Bandwidth Between the Ingress Queues” section on page 34-89, the “Configuring SRR Shaped Weights on an Egress Queue-Set” section on page 34-95, and the “Configuring SRR Shared Weights on an Egress Queue-Set” section on page 34-96.

**Queueing and Scheduling of Ingress Queues**

Figure 34-8 shows the ingress queueing and scheduling flowchart.

![Ingress Queueing and Scheduling Flowchart](image)

**Note**

SRR services the priority queue for its configured share before servicing the other queue.
The switch supports two configurable ingress queues, which are serviced by SRR in shared mode only. Table 34-2 describes the queues.

### Table 34-2 Ingress Queue Types

<table>
<thead>
<tr>
<th>Queue Type</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal</td>
<td>User traffic that is considered to be normal priority. You can configure three different thresholds to differentiate among the flows. You can use the <code>mls qos srr-queue input threshold</code>, the <code>mls qos srr-queue input dscp-map</code>, and the <code>mls qos srr-queue input cos-map</code> global configuration commands.</td>
</tr>
<tr>
<td>Expedite</td>
<td>High-priority user traffic such as differentiated services expedited forwarding or voice traffic. You can configure the bandwidth required for this traffic as a percentage of the total traffic by using the <code>mls qos srr-queue input priority-queue</code> global configuration command. The expedite queue has guaranteed bandwidth.</td>
</tr>
</tbody>
</table>

1. The switch uses two nonconfigurable queues for traffic that is essential for proper network operation.

You assign each packet that flows through the switch to a queue and to a threshold. Specifically, you map DSCP or CoS values to an ingress queue and map DSCP or CoS values to a threshold ID. You use the `mls qos srr-queue input dscp-map queue queue-id {dscp1...dscp8 | threshold threshold-id dscp1...dscp8}` or the `mls qos srr-queue input cos-map queue queue-id {cos1...cos8 | threshold threshold-id cos1...cos8}` global configuration command. You can display the DSCP input queue threshold map and the CoS input queue threshold map by using the `show mls qos maps` privileged EXEC command. To specify the queue and threshold values for CPU-generated traffic, you use the `mls qos srr-queue output cpu queue-id threshold-id` global configuration command.

### WTD Thresholds

The queues use WTD to support distinct drop percentages for different traffic classes. Each queue has three drop thresholds: two configurable (explicit) WTD thresholds and one nonconfigurable (implicit) threshold preset to the queue-full state. You assign the two explicit WTD threshold percentages for threshold ID 1 and ID 2 to the ingress queues by using the `mls qos srr-queue input threshold queue-id {threshold-percentage1 threshold-percentage2}` global configuration command. Each threshold value is a percentage of the total number of allocated buffers for the queue. The drop threshold for threshold ID 3 is preset to the queue-full state, and you cannot modify it. For more information about how WTD works, see the “Weighted Tail Drop” section on page 34-19.

### Buffer and Bandwidth Allocation

You define the ratio (allocate the amount of space) with which to divide the ingress buffers between the two queues by using the `mls qos srr-queue input buffers percentage1 percentage2` global configuration command. The buffer allocation together with the bandwidth allocation control how much data can be buffered and sent before packets are dropped. You allocate bandwidth as a percentage by using the `mls qos srr-queue input bandwidth weight1 weight2` global configuration command. The ratio of the weights is the ratio of the frequency in which the SRR scheduler sends packets from each queue to the internal ring.
Priority Queueing

You can configure one ingress queue as the priority queue by using the `mls qos srr-queue input priority-queue queue-id bandwidth weight` global configuration command. The priority queue should be used for traffic (such as voice) that requires guaranteed delivery because this queue is guaranteed part of the bandwidth regardless of the load on the internal ring.

SRR services the priority queue for its configured weight as specified by the `bandwidth` keyword in the `mls qos srr-queue input priority-queue queue-id bandwidth weight` global configuration command. Then, SRR shares the remaining bandwidth with both ingress queues and services them as specified by the weights configured with the `mls qos srr-queue input bandwidth weight1 weight2` global configuration command.

You can combine the commands described in this section to prioritize traffic by placing packets with particular DSCP or CoS values into certain queues, by allocating a large queue size or by servicing the queue more frequently, and by adjusting queue thresholds so that packets with lower priorities are dropped. For configuration information, see the “Configuring Ingress Queue Characteristics” section on page 34-86.

Queueing and Scheduling of Egress Queue-Sets

Figure 34-9 shows the egress queue-set queueing and scheduling flowchart.
Note

If the egress priority queue is enabled on a port, SRR services it until it is empty. Then SRR services the other queues.

Each port supports four egress queues, one (queue 1) of which can be the egress priority queue. These queues are assigned to a queue-set. All traffic exiting the switch on a standard port flows through one of these four queues and is subjected to a threshold based on the QoS label assigned to the packet. Traffic destined for an ES port passes through the queue-set before reaching the hierarchical queues. If congestion occurs in the hierarchical queues that backs up to the queue-sets, the queue-set configuration controls how traffic is dropped.
Figure 34-10 shows the egress queue-set buffer. The buffer space is divided between the common pool and the reserved pool. The switch uses a buffer allocation scheme to reserve a minimum amount of buffers for each egress queue, to prevent any queue or port from consuming all the buffers and depriving other queues, and to control whether to grant buffer space to a requesting queue. The switch detects whether or not the target queue has consumed more buffers than its reserved amount (under-limit), whether it has consumed all of its maximum buffers (over limit), and whether the common pool is empty (no free buffers) or not empty (free buffers). If the queue is not over-limit, the switch can allocate buffer space from the reserved pool or from the common pool (if it is not empty). If there are no free buffers in the common pool or if the queue is over-limit, the switch drops the frame.

Figure 34-10  Egress Queue-Set Buffer Allocation

### Buffer and Memory Allocation

You guarantee the availability of buffers, set drop thresholds, and configure the maximum memory allocation for a queue-set by using the `mls qos queue-set output qset-id threshold queue-id drop-threshold1 drop-threshold2 reserved-threshold maximum-threshold` global configuration command. Each threshold value is a percentage of the queue’s allocated memory, which you specify by using the `mls qos queue-set output qset-id buffers allocation1 ... allocation4` global configuration command. The sum of all the allocated buffers represents the reserved pool, and the remaining buffers are part of the common pool.

Through buffer allocation, you can ensure that high-priority traffic is buffered. For example, if the buffer space is 400, you can allocate 70 percent of it to queue 1 and 10 percent to queues 2 through 4. Queue 1 then has 280 buffers allocated to it, and queues 2 through 4 each have 40 buffers allocated to them.

You can guarantee that the allocated buffers are reserved for a specific queue in a queue-set. For example, if there are 100 buffers for a queue, you can reserve 50 percent (50 buffers). The switch returns the remaining 50 buffers to the common pool. You also can enable a queue in the full condition to obtain more buffers than are reserved for it by setting a maximum threshold. The switch can allocate the needed buffers from the common pool if the common pool is not empty.

### WTD Thresholds

You can assign each packet that flows through the switch to a queue and to a threshold. Specifically, you map DSCP or CoS values to an egress queue-set and map DSCP or CoS values to a threshold ID. You use the `mls qos srr-queue output dscp-map queue queue-id {dscp1...dscp8} threshold threshold-id dscp1...dscp8` or the `mls qos srr-queue output cos-map queue queue-id {cos1...cos8} threshold threshold-id cos1...cos8` global configuration command. You can display the DSCP output queue
threshold map and the CoS output queue threshold map by using the `show mls qos maps` privileged EXEC command. To specify the queue and threshold values for CPU-generated traffic, you use the `mls qos srr-queue output cpu queue id threshold id` global configuration command.

The queue-set uses WTD to support distinct drop percentages for different traffic classes. Each queue has three drop thresholds: two configurable (*explicit*) WTD thresholds and one nonconfigurable (*implicit*) threshold preset to the queue-full state. You assign the two WTD threshold percentages for threshold ID 1 and ID 2. The drop threshold for threshold ID 3 is preset to the queue-full state, and you cannot modify it. For more information about how WTD works, see the “Weighted Tail Drop” section on page 34-19.

**Shaped or Shared Mode**

SRR services each queue-set in shared or shaped mode. You map a port to a queue-set by using the `queue-set qset-id` interface configuration command. You assign shared or shaped weights to a standard port by using the `srr-queue bandwidth share weight1 weight2 weight3 weight4` or the `srr-queue bandwidth shape weight1 weight2 weight3 weight4` interface configuration command. You can assign only shared weights to an ES port. For an explanation of the differences between shaping and sharing, see the “SRR Shaping and Sharing” section on page 34-19.

The buffer allocation together with the SRR weight ratios control how much data can be buffered and sent before packets are dropped. The weight ratio is the ratio of the frequency in which the SRR scheduler sends packets from each queue.

All four queues participate in the SRR unless the egress priority queue is enabled, in which case the first bandwidth weight is ignored and is not used in the ratio calculation. Before servicing the other queues, SRR services the priority queue until it is empty. You enable the priority queue by using the `priority-queue out` interface configuration command.

You can combine the commands described in this section to prioritize traffic by placing packets with particular DSCP or CoS values into certain queues, by allocating a large queue size or by servicing the queue more frequently, and by adjusting queue thresholds so that packets with lower priorities are dropped. For configuration information, see the “Configuring Egress Queue-Set Characteristics” section on page 34-91.

**Note**
The egress queue-set settings are suitable for most situations. You should change them only when you have a thorough understanding of the queues and only if these settings do not meet your QoS solution.

**QoS Treatment for Performance-Monitoring Protocols**

- Cisco IP-SLAs, page 34-26
- Two-Way Active Measurement Protocol, page 34-26
- QoS Treatment for IP-SLA and TWAMP Probes, page 34-26
- QoS Marking for CPU-Generated Traffic, page 34-27
- QoS Queuing for CPU-Generated Traffic, page 34-28
- Configuration Guidelines, page 34-29
Cisco IP-SLAS

For information about Cisco IP service level agreements (IP SLAs), see the “Understanding Cisco IOS IP SLAs” section on page 41-1.

Two-Way Active Measurement Protocol

For information about the Two-Way Active Measurement Protocol (TWAMP), see:

- “Understanding TWAMP” section on page 41-14
- “Configuring TWAMP” section on page 41-15

QoS Treatment for IP-SLA and TWAMP Probes

The QoS treatment for IP-SLA and TWAMP probes must exactly reflect the effects that occur to the normal data traffic crossing the device.

The generating device should not change the probe markings. It should queue these probes based on the configured queueing policies for normal traffic.

Marking

By default, the class of service (CoS) marking of CFM traffic (including IP SLAs using CFM probes) is not changed. This feature cannot change this behavior.

By default, the class of service (CoS) marking of all other Layer 2 non-IP traffic is not changed. The QoS marking feature can change this behavior.

By default, IP traffic marking (including IP SLA and TWAMP probes) is not changed. The QoS marking feature can change this behavior.

Queuing

The CFM traffic (including IP SLAs using CFM probes) is queued according to its CoS value and the output policy map configured on the egress port, similar to normal traffic. This feature cannot change this behavior.

By default, all other Layer 2 non-IP traffic is statically mapped to a queue on the egress port. However, this feature can change the queuing behavior. This traffic can be queued according to the CoS markings specified in the `cpu traffic qos global` configuration command and the global CoS-to-queue mapping.

By default, all IP traffic (including IP SLA and TWAMP probes) is statically mapped to a queue on the egress port. However, this feature can change the queuing behavior. All IP traffic can be queued according to the CoS or DSCP or precedence markings specified in the `cpu traffic qos global` configuration command and the corresponding global CoS- or DSCP- or precedence-to-queue mapping.

Note

This feature enhances the MLS QoS marking and queuing capability for CPU traffic. It does not affect the marking and queuing capability availability through output MQC QoS policy-maps configured on enhanced services (ES) ports.
QoS Marking for CPU-Generated Traffic

Beginning with Cisco IOS Release 12.2(52)SE, you can use QoS marking to set or modify the attributes of traffic from the CPU. The QoS marking action can cause the CoS, IP DSCP, or IP precedence bits in the packet to be rewritten or left unchanged. QoS uses packet markings to identify certain traffic types and how QoS treats them on the local switch and the network.

Note
To configure QoS marking, you must first enable multilayer switch (MLS) QoS by using the mls qos global configuration command.

When MLS QoS is disabled, the default behavior applies for all CPU traffic; QoS marking commands are accepted by the switch and become effective when MLS QoS is enabled.

You can specify and mark traffic CPU-generated traffic by using these global configuration commands:

- `cpu traffic qos cos {cos_value | trust}`
- `cpu traffic qos dscp {dscp_value | trust | dscp-mutation mutation-map-name}`
- `cpu traffic qos precedence {precedence_value | trust | precedence-mutation mutation-map-name}`

For non-IP, non-CFM CPU traffic, you have these marking options:

- Use the `cpu traffic qos cos` global configuration command with the `cos_value` argument to configure a CoS value.
- Use the `cpu traffic qos cos` global configuration command with the `trust` keyword to trust the CoS value in the inbound frame and use the configurable CoS-to-DSCP map to generate a DSCP value for the packet.

Note
Configuring a DSCP or precedence value or trusting the DSCP or precedence value in the inbound frame has no impact on non-IP traffic.

For IP CPU traffic, you have these marking options:

- Use the `cpu traffic qos cos` global configuration command with the `cos_value` argument to configure a CoS value.
- Use the `cpu traffic qos cos` global configuration command with the `trust` keyword to trust the CoS value in the inbound frame and use the configurable CoS-to-DSCP map to generate a DSCP value for the packet.
- Use the `cpu traffic qos dscp` global configuration command with the `dscp_value` argument to configure the DSCP value.
- Use the `cpu traffic qos dscp` global configuration command with the `trust` keyword to trust the DSCP value in the inbound frame and use the configurable DSCP-to-CoS map to generate a CoS value for the packet.
- Use the `cpu traffic qos dscp` global configuration command with the `dscp-mutation` keyword and `mutation-map-name` argument to change the DSCP value of the inbound frame and use the configurable DSCP-to-CoS map to generate a CoS value for the packet.
- Use the `cpu traffic qos precedence` global configuration command with the `precedence_value` argument to configure the precedence value.
• Use the `cpu traffic qos precedence` global configuration command with the `trust` keyword to trust the precedence value in the inbound frame, use the configurable IP-precedence-to-DSCP map to generate a DSCP value, and use the configurable DSCP-to-CoS map to generate a CoS value for the packet.

• Use the `cpu traffic qos precedence` global configuration command with the `precedence-mutation` keyword and the `mutation-map-name` argument to change the precedence value of the inbound frame. Use the IP-precedence-to-DSCP map to generate a DSCP value from the precedence value, and then use the configured DSCP mutation-map to generate the changed DSCP value. Use the configurable DSCP-to-CoS map to generate a CoS value for the packet.

### QoS Queuing for CPU-Generated Traffic

Both the QoS markings configured for the CPU-generated traffic by the `cpu traffic qos` global configuration command and the global QoS marking-to-queue mapping identify the queue on the egress port.

By default, CPU traffic is assigned to queue-2, threshold-1.

For CFM CPU traffic you have this queuing option:

• Use the `cpu traffic qos cos` global configuration command with the `trust` keyword to trust the CoS value in the inbound frame, and use the configurable CoS-to-queue or CoS-to-threshold map to select the queue or threshold for the packet.

For all non-CFM CPU traffic, you have this queuing option:

• Use the `mls qos srr-queue output cpu-queue` global configuration command to specify an egress queue and a threshold value.

For non-IP, non-CFM CPU traffic, you have these queuing options:

• Use the `cpu traffic qos cos` global configuration command with the `cos_value` argument to configure a CoS value. Then use the configurable CoS-to-queue or CoS-to-threshold map to select the queue or threshold for the packet.

• Use the `cpu traffic qos cos` global configuration command with the `trust` keyword to trust the CoS value in the inbound frame, and use the configurable CoS-to-queue or CoS-to-threshold map to select the queue or threshold for the packet.

• Use the `cpu traffic qos dscp` global configuration command with the `dscp_value` argument to configure the DSCP value. Then use the configurable DSCP-to-queue or DSCP-to-threshold map to select the queue or threshold for the packet.

---

**Note**

The DSCP-to-queue map has no impact on non-IP traffic.

For IP CPU traffic, you have these queuing options:

• Use the `cpu traffic qos cos` global configuration command with the `cos_value` argument to configure a CoS value. Then use the configurable CoS-to-queue or CoS-to-threshold map to select the queue or threshold for the packet.

• Use the `cpu traffic qos cos` global configuration command with the `trust` keyword to trust the CoS value in the inbound frame, then use the configurable CoS-to-queue or CoS-to-threshold map to select the queue or threshold for the packet.

• Use the `cpu traffic qos dscp` global configuration command with the `dscp_value` argument to configure the DSCP value. Then use the configurable DSCP-to-queue or DSCP-to-threshold map to select the queue or threshold for the packet.
• Use the `cpu traffic qos dscp` global configuration command with the `trust` keyword to trust the DSCP value in the inbound frame. Then use the configurable DSCP-to-queue or DSCP-to-threshold map to select the queue or threshold for the packet.

• Use the `cpu traffic qos dscp` global configuration command with the `dscp-mutation` keyword and `mutation-map-name` argument to change the DSCP value of the inbound frame. Then use the configurable DSCP-to-queue or DSCP-to-threshold map to select the queue or threshold for the packet.

• Use the `cpu traffic qos precedence` global configuration command with the `precedence_value` argument to configure the precedence value. Then use the configurable DSCP-to-queue or DSCP-to-threshold map to select the queue or threshold for the packet.

• Use the `cpu traffic qos precedence` global configuration command with the `trust` keyword to trust the precedence value in the inbound frame. Then use the configurable IP-precedence-to-DSCP map to generate a DSCP value. Use the configurable DSCP-to-queue or DSCP-to-threshold map to select the queue or threshold for the packet.

• Use the `cpu traffic qos precedence` global configuration command with the `precedence-mutation` keyword and the `mutation-map-name` argument to change the precedence value of the inbound frame. Use the IP-precedence-to-DSCP map to generate a DSCP value from the precedence value. Then use the configured DSCP mutation-map to generate the changed DSCP value. Then use the configurable DSCP-to-queue or DSCP-to-threshold map to select the queue or threshold for the packet.

**Configuration Guidelines**

• This feature must be configured globally for a switch; it cannot be configured per-port or per-protocol.

• Enter each `cpu traffic qos` marking action on a separate line.

• The `trust` keyword configures the switch to trust the incoming CoS, DSCP, or precedence value and marks the packet according to the global map configuration.

• The `mutation` keyword configures the switch to change the incoming value according to the global mutation-map configuration.

• When you configure the switch to trust CoS, the configuration applies to both IP and non-IP traffic.

• When you configure the switch to trust or change DSCP or precedence but not CoS, the configuration applies only to IP traffic.

• When you configure the switch to trust CoS and trust or change DSCP or precedence, trust CoS applies to non-IP traffic and trust or change DSCP or precedence applies to IP traffic.

• The `cpu traffic qos cos` global configuration command configures CoS marking for CPU-generated traffic by either trusting CoS or specifying a CoS value, but not both. A new configuration overwrites the existing configuration.

• The `cpu traffic qos dscp` global configuration command configures DSCP marking for CPU-generated traffic by trusting DSCP, mutating DSCP, or specifying a DSCP value. A new configuration overwrites the existing configuration.

• The `cpu traffic qos precedence` global configuration command configures precedence marking for CPU-generated traffic by trusting precedence, mutating precedence, or specifying a precedence value. A new configuration overwrites the existing configuration.

• The `cpu traffic qos dscp` and `cpu traffic qos precedence` global configuration commands are mutually exclusive. A new configuration overwrites the existing configuration.
Understanding Hierarchical QoS

The switch supports a hierarchical QoS configuration (traffic classification, CBWFQ, LLQ, shaping, and two-rate three-color policing) that is applied to the input or to the output of an ES port. Beginning with Cisco IOS Release 12.2(35)SE, it also supports input and output hierarchical QoS on an EtherChannel made of ES ports.

Hierarchical QoS configuration is based on the concept of a bandwidth-limited stream of traffic, which is a stream of packets that has its departure rate constrained in some manner. At each level of the hierarchy, the switch must classify each packet to select into which traffic stream in that level the packet belongs. When the stream is classified, if its arrival rate exceeds its departure rate, queueing can become congested. To compensate for this, you can configure policies that contain policer drops, configure tail drop or WRED, a congestion-avoidance technique, or to influence whether the packet is queued. You also can implement scheduling policies (CBWFQ, LLQ, and shaping) to influence how quickly a packet is sent out the port.

This section includes these topics:

- Hierarchical Levels, page 34-30
- Hierarchical Classification Based on Traffic Classes and Traffic Policies, page 34-33
- Hierarchical Policies and Marking, page 34-34
- Queueing and Scheduling of Hierarchical Queues, page 34-37

Hierarchical Levels

Hierarchical QoS configuration involves traffic classification, policing, queueing, and scheduling. You can create a hierarchy by associating a class-level policy map with a VLAN-level policy map, by associating that VLAN-level policy map with a physical-level policy map, and by attaching the physical-level policy map to an ES port. You can omit hierarchical levels, but the order of the levels (class level, VLAN level, and then the physical level) must be preserved.

You can configure these three QoS levels in the hierarchy:

- Class level—You configure this level of the hierarchy by matching CoS, DSCP, IP precedence, or MPLS EXP bits in the outbound packet through the `match { cos [inner] | dscp | ip precedence | mpls experimental }` class-map configuration command. At the class level, you can:
  - Configure policer drops by using the `police cir` or `police cir percent` policy-map class configuration command.
  - Configure tail drop or WRED drop policies by using the `queue-limit` or the `random-detect` policy-map class configuration command.
  - Modify the traffic class by setting Layer 2 and Layer 3 QoS fields through the `set { cos | dscp | precedence | mpls experimental }` policy-map class configuration command.
- Configure CBWFQ or LLQ scheduling by using the **bandwidth** or the **priority** policy-map class configuration command.

- Configure traffic shaping by using the **shape** policy-map class configuration command.

The switch supports eight classes (including the class) per policy map at this level. The class is reserved for packets that do not meet any of the matching criteria.

This is an example of a class-level classification and its naming convention:

```text
Switch(config)# class-map match-any class-level-class-map-name
Switch(config-cmap)# match ip dscp 10 11 12
```

This is an example of a class-level policy map and its naming convention:

```text
Switch(config)# policy-map class-level-policy-map-name
Switch(config-pmap)# class class-level-class-name
Switch(config-pmap-c)# bandwidth percent 20
Switch(config-pmap-c)# shape average 20000000
```

This is a class-level configuration example that combines a class-level classification and a class-level policy map to create a service policy:

```text
Switch(config)# class-map c1
Switch(config-cmap)# match ip precedence 4
Switch(config-cmap)# exit
Switch(config)# policy-map policy1
Switch(config-pmap)# class c1
Switch(config-pmap-c)# police cir 500000 bc 10000 pir 1000000 be 10000 conform-action transmit exceed-action set-prec-transmit 2 violate-action drop
Switch(config-pmap-c)# exit
Switch(config)# interface gigabitethernet1/1/1
Switch(config-if)# service-policy output policy1
```

- **VLAN level**—You start configuration of per-VLAN QoS by entering the **match vlan vlan-id** class-map configuration command on one or more VLANs or by entering the **match vlan vlan-id** and the **match vlan inner vlan-id** class-map configuration command on one or more 802.1Q tunnels. At this level, you can configure the VLANs or 802.1Q tunnels to police, to share the available port bandwidth and to enable CBWFQ, and to shape the traffic. You configure these features by using the **police cir**, **police cir percent**, **bandwidth**, and **shape** policy-map class configuration commands.

  For a finer level of control, you can associate a previously defined child policy at the class level with a new service policy by using the **service-policy** policy-map class configuration command. In the class-level child policy, you can configure tail drop or WRED drop policies, set Layer 2 and Layer 3 QoS fields, or enable the strict-priority queue. These features are available only at the class level. By using a child policy, you apply a class-level policy only to traffic that matches the VLAN class.

  You cannot mix VLAN-level and class-level matches within a class map.

  You can attach up to 2045 user-created VLAN-level classes. This means that you can have 1022 unique classes and can associate them with the two ES ports (and have one left over), or you can add more classes to one ES port and can subtract from the other one. You can shape every class that you configure. You can create up to 4093 class maps.

This is an example of a VLAN-level classification and its naming convention:

```text
Switch(config)# class-map match-all vlan-level-class-map-name
Switch(config-cmap)# match vlan 5
Switch(config-cmap)# match vlan inner 3 - 8
```

This is an example of a VLAN-level policy map and its naming convention:
Switch(config)# policy-map vlan-level-policy-map-name
Switch(config-pmap)# class vlan-level-class-name
Switch(config-pmap-c)# police cir 500000 bc 10000 pir 1000000 be 10000 conform-action
transmit exceed-action set-prec-transmit 2 violate-action drop

This is an example of a VLAN-level policy map and its naming convention when a previously defined child policy is associated at the class level:

Switch(config)# policy-map vlan-level-policy-map-name
Switch(config-pmap)# class vlan-level-class-name
Switch(config-pmap-c)# bandwidth percent 30
Switch(config-pmap-c)# service-policy class-level-policy-map-name

This is a VLAN-level configuration example that combines a VLAN-level classification and a VLAN-level policy map:

Switch(config)# class-map match-all vlan203
Switch(config-cmap)# match vlan 203
Switch(config-cmap)# exit
Switch(config)# policy-map vlan-policy
Switch(config-pmap)# class vlan203
Switch(config-pmap-c)# police cir 500000 bc 10000 pir 1000000 be 10000 conform-action
transmit exceed-action set-prec-transmit 2 violate-action drop

This is an example of a VLAN-level policy map that combines a VLAN-level classification with a VLAN-level policy map and associates a previously defined child policy at the class level:

Switch(config)# class-map cls-class
Switch(config-cmap)# match mpls experimental 2
Switch(config-cmap)# exit
Switch(config)# class-map log-class
Switch(config-cmap)# match vlan 203
Switch(config-cmap)# exit
Switch(config)# policy-map cls-policy
Switch(config-pmap)# class cls-class
Switch(config-pmap-c)# set mpls experimental 5
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet1/1/2
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# service-policy output log-policy

- Physical level—You can shape or police only the class-default class at the physical level of the hierarchy by using the shape, police cir, or police cir percent policy-map class configuration command.

Within a policy map, the class-default applies to all traffic that is not explicitly matched within the policy map but does match the parent policy. If no parent policy is configured, the parent policy represents the physical port. In a physical-level policy map, class-default is the only class that you can configure.

You use the service-policy [input | output] policy-map-name interface configuration command to attach a hierarchical policy to an ES port.

This is an example of a physical-level configuration. All hierarchical levels exist, and the order is preserved. The class level at the bottom, the VLAN level in the middle, and the physical level at the top.
Switch(config)# class-map my-class
Switch(config-cmap)# match ip precedence 1
Switch(config-cmap)# exit
Switch(config)# class-map my-logical-class
Switch(config-cmap)# match vlan 5
Switch(config-cmap)# exit
Switch(config)# policy-map my-class-policy
Switch(config-pmap)# class my-class
Switch(config-pmap-c)# set precedence 2
Switch(config-pmap-c)# exit
Switch(config)# policy-map my-logical-policy
Switch(config-pmap)# class my-logical-class
Switch(config-pmap-c)# shape average 400000000
Switch(config-pmap-c)# service-policy my-class-policy
Switch(config-pmap-c)# exit
Switch(config)# policy-map my-physical-policy
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# shape average 500000000
Switch(config-pmap-c)# service-policy my-logical-policy
Switch(config-pmap-c)# exit
Switch(config)# interface gigabitethernet1/1/1
Switch(config-if)# service-policy output my-physical-policy

Hierarchical Classification Based on Traffic Classes and Traffic Policies

Hierarchical classification distinguishes one kind of traffic from another on receipt or before sending. The switch examines the fields in the packet, processes the **match** commands, and creates the queues. The switch forwards the traffic according to the QoS specifications set in the hierarchical policy.

You use the class map to define a specific traffic flow (or class) and to isolate it from all other traffic. The class map defines the criteria used to match against a specific traffic flow to further classify it. At the class level, the criteria can include matching CoS, DSCP, IP precedence, or MPLS EXP bits in the header. At the VLAN level, the criteria can include matching a packet based on the inner and the outer VLAN IDs. If you have more than one type of traffic that you want to classify, you can create another class map and use a different name.

You create a class map by using the **class-map** global configuration command. When you enter the **class-map** command, the switch enters the class-map configuration mode. In this mode, you define the match criterion for the traffic by using the **match** class-map configuration command. Packets are compared to the match criteria configured for a class map. If a packet matches the specified criteria, the packet is considered a member of the class, the switch creates a queue for it, and the packet is forwarded according to the QoS specifications set in the traffic policy. If a packet fails to meet any of the matching criteria, it is classified as a member of the traffic class if one is configured.

You use the policy map to create the traffic policy, to specify the traffic class to act on, and to configure the QoS features associated with the traffic class. Actions can include trusting the received CoS, DSCP, or IP precedence bits in the traffic class; setting specific CoS, DSCP, IP precedence, or MPLS EXP bits in the traffic class; or specifying the traffic bandwidth limitations and the action to take when the traffic is out of profile.

You create and name a policy map by using the **policy-map** global configuration command. When you enter this command, the switch enters the policy-map configuration mode. In this mode, you use the **class** policy-map configuration command to name the traffic class associated with the traffic policy. If
you specify **class-default** as the class name in the **class** policy-map configuration command, packets that fail to meet any of the matching criteria are classified as members of the traffic class. You can manipulate this class (for example, police it and mark it) just like any traffic class, but you cannot delete it.

Within a policy map, the class-default designates all traffic that is not explicitly matched within the policy map but does match the policy map of the parent policy. If no parent policy is configured, the parent policy represents the physical port. In the physical-level policy map, class-default is the only class that can be configured.

After you name the traffic class with the **class** command, the switch enters policy-map class configuration mode, and you can specify the actions to take on this traffic class.

You attach a hierarchical policy map to an ES port by using the **service-policy [input | output] policy-map-name** interface configuration command. The policy map can include the **bandwidth**, **police cir**, **police cir percent**, **priority**, **queue-limit**, **random-detect**, **shape**, or **set** policy-map class configuration commands. If the policy map contains the class-class, you can configure settings only through the **police cir**, **police cir percent**, and **shape** commands.

For more information, see the “Hierarchical Policies and Marking” section on page 34-34 and the “Queueing and Scheduling of Hierarchical Queues” section on page 34-37.

### Hierarchical Policies and Marking

Hierarchical traffic policies control the maximum rate of traffic received or sent on an ES port. A policer defines the bandwidth limitations of the traffic and the action to take if the limits are exceeded. It is often configured on ports at the edge of a network to limit traffic into or out of the network. In most policing configurations, traffic that falls within the rate parameters is sent. Traffic that exceeds the parameters is considered to be *out of profile or nonconforming* and is dropped or sent with a different priority.

You can configure a two-rate traffic policer within a policy map at the class level, at the VLAN level, and at the physical level by using the **police cir** or the **police cir percent** policy-map class configuration command. At the physical level of the hierarchy, you can police only the class-class in a policy attached to an ES port.

You can configure a two-rate traffic policer to limit the transmission rate of a traffic class and mark actions (conform, exceed, and violate) for each packet. Within the conform, exceed, and violate categories, you decide packet treatments. In the most common configurations, you configure packets that conform to be sent, packets that exceed to be sent with a decreased priority, and packets that violate to be dropped. You can decrease the priority of the CoS, the DSCP, the IP precedence, or the MPLS EXP bits in the packet.

The two-rate policer manages the maximum rate of traffic through a token-bucket algorithm. The algorithm uses the configured committed information rate (CIR) and the peak information rate (PIR) rate values to control the maximum rate of traffic allowed on a port at a given moment in time. The algorithm is affected by all traffic leaving the port, and it manages network bandwidth when several large packets are sent in the same traffic stream.

A token bucket is provided for the CIR and the PIR as shown in Figure 34-11.
You configure the CIR and PIR rates in bps (or as a percentage of the bandwidth available on an ES port), and these rates control how fast the bucket fills (is updated) with tokens. The conform burst size (bc) and the peak burst size (be) represent the depth of the CIR and PIR buckets in bytes. This depth limits the number of tokens that the bucket can accumulate. If the bucket fills to capacity, newly arriving tokens are discarded.

Each token is permission for the source to send a certain number of bits into the network. To send a packet, the number of tokens equal to the packet size must be drained from the bucket. If there are enough tokens in the bucket, the packet conforms and can pass to the next stage. Otherwise, the exceed action associated with the bucket is applied to the packet. The packet might be dropped, or its priority value might be marked down.

In this token-bucket example, if the CIR rate is 2 kb/s, 2000 tokens are added to the bucket every second (for this example, consider each token to represent a single bit of information). If a 1500-byte packet arrives, 12000 tokens (1500 bytes x 8 bits per byte) must be in the bucket for the packet to pass to the next state without triggering the exceed action. If enough tokens are in the bucket, they are drained, and the packet conforms and passes to the next stage. If there are less than 12000 tokens in the bucket, the exceed action is applied to the packet. The deeper the bucket, the more data can burst through at a rate greater than the rate at which the bucket is filling. For example, if the CIR bucket holds 6000 tokens, 750 bytes of traffic can instantaneously burst without draining the bucket (and without triggering an exceed action), even though the instantaneous burst is at a greater rate than the CIR rate of 2000 bps.

If the burst sizes approach the system maximum transmission unit (MTU), the policer strictly enforces the CIR and PIR. Normal traffic jitter can cause some percentage of inbound traffic to be flagged as nonconforming even if the average inbound rate appears to conform. If the burst size is very large, on the other hand, large traffic bursts at nonconforming data rates can be passed through the policer and flagged as conforming. Setting the burst sizes too low can result in less traffic than expected and setting them too high can result in more traffic than expected.
For packet marking actions, if the CIR is 100 kb/s, the PIR is 200 kb/s, and a data stream with a rate of 250 kb/s arrives at the two-rate policer:

- 100 kb/s is marked as conforming to the rate.
- 100 kb/s is marked as exceeding the rate.
- 50 kb/s is marked as violating the rate.

If you set the CIR equal to the PIR, a traffic rate that is less than the CIR or that meets the CIR is in the conform range. Traffic that exceeds the CIR rate is in the violate range.

If you set the PIR greater than the CIR, a traffic rate less than the CIR is in the conform range. A traffic rate that exceeds the CIR but is less than or equal to the PIR is in the exceed range. A traffic rate that exceeds the PIR is in the violate range.

After you configure the policy map and policing actions, attach the policy to an ES port by using the `service-policy {input | output} policy-map-name` interface configuration command. For configuration information, see the “Configuring Hierarchical QoS” section on page 34-103.

An input hierarchical service policy can contain the same configuration options as an output hierarchical service policy (policing, shaping, CBWFQ), but cannot include configurations such as ACLs or aggregate policers. Access group matches are allowed on ES ports if the policy is non-hierarchical. Violating this rule prevents the policy from being attached to an interface.
Queueing and Scheduling of Hierarchical Queues

Figure 34-12 shows the queueing and scheduling flowchart for a hierarchical queue.

**Figure 34-12 Queueing and Scheduling Flowchart for a Hierarchical Queue**
Hierarchical Queues

The switch uses a hierarchical queueing model for traffic received on or sent from an ES port. Each packet is assigned a queue based on its physical interface, VLAN, or class:

- At the class level, a packet is queued to one of four queues according to its CoS, DSCP, IP precedence, or MPLS EXP classification. Packets can be classified by any combination of these values, but if a packet matches more than one, the classification occurs in the order listed. The last queue in each set of four queues is reserved as the default queue. Packets that are not classified into one of the other three queues are assigned to the default queue. You can configure traffic in the queue with congestion-avoidance features and scheduling congestion-management features as described in the “Queueing and Scheduling of Hierarchical Queues” section on page 34-37.

- At the VLAN level, the switch supports 2045 VLAN classes divided between the two ES ports. One queue is reserved as the default queue. Packets that are not classified into one of the other VLAN queues are assigned to the default queue. You can configure traffic in the default queue with congestion-avoidance features and scheduling congestion-management features as described in the “Queueing and Scheduling of Hierarchical Queues” section on page 34-37.

- At the physical level, the switch reserves one queue per port. The switch creates the queue and uses it to send all traffic when a service policy is not attached to an ES port. User traffic on a physical port without an attached service policy bypasses the QoS classification and is queued to the default queue. The minimum and maximum bandwidth for the default queue is the same as the port bandwidth.

Under congested conditions, the switch discards packets for all classes configured for the same sending queue with equal probability. To achieve the full queueing capacity, there must be an equal division of traffic among the classes for each sending queue.

Congestion-Management and Congestion-Avoidance Features

You use congestion-management features to control congestion and to control the order in which packets are received on or are sent from an ES port based on the priorities assigned to those packets. You manage congestion by creating queues, by assigning packets based on the packet classification, and by scheduling the packets to be sent from the queue.

During periods with light traffic (when no congestion exists), the switch sends packets as soon as they arrive. During periods of congestion at the inbound or at the outbound port, packets arrive faster than the port can send them. If you use congestion-management features, the switch queues accumulating packets at a port until it is free to send them. They are then scheduled for transmission according to their assigned priorities and the queueing mechanism for the port.

You can configure either tail drop or WRED. You cannot configure both tail drop and WRED in the same class policy, but they can be used in two different class policies in the same policy map.

You can configure CBWFQ as a queue scheduling management feature, LLQ as a scheduling congestion-management feature, and traffic shaping to decrease the burstiness of traffic.

Tail Drop

With tail drop, packets are queued for the class until the maximum threshold is exceeded, and then all the packets destined for the class queue are dropped. You enable tail drop at the class level by using the queue-limit policy-map class configuration command. For configuration information, see the “Configuring a Hierarchical QoS Policy” section on page 34-107.
WRED

Cisco Systems implements a version of Random Early Detection (RED), called WRED, differently from other congestion-avoidance techniques. WRED attempts to anticipate and avoid congestion, rather than controlling congestion when it occurs. WRED takes advantage of the TCP congestion control to try to control the average queue size by signaling end hosts when they should temporarily stop sending packets. By randomly dropping packets before periods of high congestion, it tells the packet source to decrease its sending rate. Assuming the packet source is using TCP, WRED tells it to decrease its sending rate until all the packets reach their destination, meaning that the congestion is cleared. By dropping some packets early rather than waiting until the queue is full, WRED avoids dropping large numbers of packets at once.

When a packet arrives and WRED is enabled, these events occur:

- The average queue size is calculated based on the previous average and the current size of the queue. The average queue-size calculation is affected by the exponential weight constant setting in the random-detect exponential-weight-constant policy-map class configuration command.
- If the average queue size is less than the minimum queue threshold, the arriving packet is queued. The minimum queue threshold is configured through the min-threshold option in the random-detect {dscp | precedence} policy-map class configuration command.
- If the average queue size is between the minimum queue threshold and the maximum queue threshold, the packet is either dropped or queued, depending on the packet-drop probability. The packet-drop probability is based on the minimum threshold, the maximum threshold, and the mark-probability denominator. The maximum queue threshold is configured through the max-threshold option, and the mark-probability denominator is configured through the mark-prob-denominator option in the random-detect dscp {dscp | precedence} policy-map class configuration command.
- If the average queue size is greater than the maximum queue threshold, the packet is automatically dropped.

You enable WRED by using the random-detect policy-map class configuration command at the class level. This command allows for preferential drop treatment among packets with different IP precedence or DSCP values. The WRED algorithm discards or marks packets destined for a queue when that queue is congested. It discards packets fairly and before the queue is full. Packets with high IP-precedence values are preferred over packets with low IP-precedence values. For configuration information, see the “Configuring a Hierarchical QoS Policy” section on page 34-107.

CBWFQ

CBWFQ provides guaranteed bandwidth to particular traffic classes, such as voice, that are delay sensitive, while still fairly serving all other traffic in the network. You define traffic classes based on match criteria. Packets satisfying the match criteria for a class constitute the traffic for that class. A queue is reserved for each class, and traffic belonging to a class is directed to the queue for that class. The bandwidth assigned to a class is the minimum bandwidth that is delivered to the class during congestion. CBWFQ uses the bandwidth weight to ensure that the queue for the class is serviced fairly.

You enable CBWFQ and specify the minimum bandwidth as a rate in kb/s or as a percentage of the available bandwidth by using the bandwidth policy-map class configuration command at the class level or at the VLAN level. During periods of congestion, the classes are serviced in proportion to their configured bandwidth. The amount of bandwidth available to a class is dependent on the amount of bandwidth reserved by the parent class. For configuration information, see the “Configuring a Hierarchical QoS Policy” section on page 34-107.
Chapter 34 Configuring QoS

LLQ

LLQ provides strict-priority queueing for a traffic class. It enables delay-sensitive data, such as voice, to be sent before packets in other queues are sent. The priority queue is serviced first until it is empty. Only one traffic stream can be destined for the priority queue per class-level policy. The priority queue restricts all traffic streams in the same hierarchy, and you should use care when configuring this feature. You enable the priority queue for a traffic class by using the priority policy-map class configuration command at the class level. For configuration information, see the “Configuring a Hierarchical QoS Policy” section on page 34-107.

With Cisco IOS Release 12.1(14)AX2, you can use LLQ and the egress priority queue (enabled with the priority-queue out interface configuration command) to give priority to a class of traffic and to avoid a loss of traffic when the switch is congested. In previous releases (before the egress priority queue was supported), you could put a traffic class into the strict-priority queue, but congestion at the egress queue-sets could result in the dropping of that priority traffic. You can use the priority-queue out interface configuration command to prioritize the same traffic class at the egress queue-sets, ensuring that priority traffic reaches the hierarchical queues and is processed with priority.

Shaping

Shaping provides a process for delaying out-of-profile packets in queues so that they conform to a specified profile. Shaping is distinct from policing. Policing drops packets that exceed a configured threshold, but shaping buffers packets so that traffic remains within a threshold. Shaping offers greater smoothness in handling traffic than policing. You enable average-rate traffic shaping on a traffic class by using the shape policy-map class configuration command at the class level or at the VLAN level. At the physical level of the hierarchy, you can shape only the class-default class by using the shape policy-map class configuration command in a policy attached to an ES port. For configuration information, see the “Configuring a Hierarchical QoS Policy” section on page 34-107.

Hierarchical QoS on EtherChannels

Beginning with Cisco IOS Release 12.2(35)SE, you can configure three-level hierarchical QoS on EtherChannels with no ports or with one or both ES ports. If you configure hierarchical QoS on an EtherChannel with no ports and add a standard port to the EtherChannel, the hierarchical policy map is removed from the EtherChannel. Hierarchical policies are not supported on a non-ES port.

For a list of differences between hierarchical QoS over EtherChannels and hierarchical QoS over ES ports, see the “Hierarchical QoS Configuration Guidelines” section on page 34-103.

Configuring Auto-QoS

You can use the auto-QoS feature to simplify the deployment of existing QoS features. Auto-QoS makes assumptions about the network design, and as a result, the switch can prioritize different traffic flows and appropriately use the ingress and egress queues instead of using the QoS behavior. The default is that QoS is disabled. The switch then offers best-effort service to each packet, regardless of the packet contents or size, and sends it from a single queue.

When you enable auto-QoS, it automatically classifies traffic based on the traffic type and ingress packet label. The switch uses the resulting classification to choose the appropriate egress queue.
You use auto-QoS commands to identify ports connected to Cisco IP Phones and to devices running the Cisco SoftPhone application. You also use the commands to identify ports that receive trusted traffic through an uplink. Auto-QoS then performs these functions:

- Detects the presence or absence of IP phones
- Configures QoS classification
- Configures egress queues

These sections describe how to configure auto-QoS on your switch:

- Generated Auto-QoS Configuration, page 34-41
- Effects of Auto-QoS on the Configuration, page 34-45
- Auto-QoS Configuration Guidelines, page 34-45
- Upgrading from a Previous Software Release, page 34-46
- Enabling Auto-QoS for VoIP, page 34-46
- Auto-QoS Configuration Example, page 34-48

### Generated Auto-QoS Configuration

By default, auto-QoS is disabled on all ports.

When auto-QoS is enabled, it uses the ingress packet label to categorize traffic, to assign packet labels, and to configure the ingress queues and egress queue-sets as shown in Table 34-3.

<table>
<thead>
<tr>
<th>Table 34-3 Traffic Types, Packet Labels, and Queues</th>
</tr>
</thead>
<tbody>
<tr>
<td>VoIP(^1) Data Traffic</td>
</tr>
<tr>
<td>DSCP</td>
</tr>
<tr>
<td>CoS</td>
</tr>
<tr>
<td>CoS-to-Ingress Queue Map</td>
</tr>
<tr>
<td>CoS-to-Egress Queue Map</td>
</tr>
</tbody>
</table>

---

1. VoIP = voice over IP.

Table 34-4 shows the generated auto-QoS configuration for the ingress queues.

<table>
<thead>
<tr>
<th>Table 34-4 Auto-QoS Configuration for the Ingress Queues</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingress Queue</td>
</tr>
<tr>
<td>SRR shared</td>
</tr>
<tr>
<td>Priority</td>
</tr>
</tbody>
</table>
Table 34-5 shows the generated auto-QoS configuration for the egress queue-set.

**Table 34-5 Auto-QoS Configuration for the Egress Queue-Set**

<table>
<thead>
<tr>
<th>Egress Queue</th>
<th>Queue Number in the Queue-Set</th>
<th>CoS-to-Queue Map</th>
<th>Queue Weight (Bandwidth)</th>
<th>Queue (Buffer) Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority (shaped)</td>
<td>1</td>
<td>5</td>
<td>10 percent</td>
<td>10 percent</td>
</tr>
<tr>
<td>SRR shared</td>
<td>2</td>
<td>3, 6, 7</td>
<td>10 percent</td>
<td>10 percent</td>
</tr>
<tr>
<td>SRR shared</td>
<td>3</td>
<td>2, 4</td>
<td>60 percent</td>
<td>26 percent</td>
</tr>
<tr>
<td>SRR shared</td>
<td>4</td>
<td>0, 1</td>
<td>20 percent</td>
<td>54 percent</td>
</tr>
</tbody>
</table>

You must enable QoS by entering the `mls qos` global configuration command before configuring the QoS parameters for CPU-generated traffic. Otherwise, the CPU traffic QoS command configurations are not applied. To configure the QoS parameters, use the `cpu traffic qos` global configuration command.

When you enable the auto-QoS feature on the first port, these automatic actions occur:

- QoS is globally enabled (`mls qos` global configuration command), and other global configuration commands are added.

  - When you enter the `auto qos voip cisco-phone` interface configuration command on a port at the edge of the network that is connected to a Cisco IP phone, the switch enables the trusted boundary feature. The switch uses the Cisco Discovery Protocol (CDP) to detect the presence or absence of a Cisco IP Phone. When a Cisco IP Phone is detected, the ingress classification on the port is set to trust the QoS label received in the packet. When a Cisco IP Phone is absent, the ingress classification is set to not trust the QoS label in the packet. The switch configures ingress queues and the egress queue-set on the port according to the settings in Table 34-4 and Table 34-5.

  - When you enter the `auto qos voip cisco-softphone` interface configuration command on a port at the edge of the network that is connected to a device running the Cisco SoftPhone, the switch uses policing to determine whether a packet is in or out of profile and to specify the action on the packet. If the packet does not have a DSCP value of 24, 26, or 46 or is out of profile, the switch changes the DSCP value to 0. The switch configures ingress and egress queues on the port according to the settings in Table 34-4 and Table 34-5.

  - When you enter the `auto qos voip trust` interface configuration command on a port connected to the interior of the network, the switch trusts the CoS value for nonrouted ports or the DSCP value for routed ports in ingress packets (the assumption is that traffic has already been classified by other edge devices). The switch configures the ingress queues and the egress queue-set on the port according to the settings in Table 34-4 and Table 34-5.

  For information about the trusted boundary feature, see the “Configuring a Trusted Boundary to Ensure Port Security” section on page 34-60.

When you enable auto-QoS by using the `auto qos voip cisco-phone`, the `auto qos voip cisco-softphone`, or the `auto qos voip trust` interface configuration command, the switch automatically generates a QoS configuration based on the traffic type and the ingress packet label and applies the commands listed in Table 34-6 to the port.

On an ES port, the `srr-queue bandwidth shape` interface configuration command is not part of the generated `auto qos voip` command list.
Table 34-6  Generated Auto-QoS Configuration

<table>
<thead>
<tr>
<th>Description</th>
<th>Automatically Generated Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>The switch automatically enables standard QoS and configures the CoS-to-DSCP map (maps CoS values in inbound packets to a DSCP value).</td>
<td>Switch(config)# mls qos Switch(config)# mls qos map cos-dscp 0 8 16 26 32 46 48 56</td>
</tr>
<tr>
<td>The switch automatically maps CoS values to an ingress queue and to a threshold ID.</td>
<td>Switch(config)# no mls qos srr-queue input cos-map Switch(config)# mls qos srr-queue input cos-map queue 1 threshold 3 0 Switch(config)# mls qos srr-queue input cos-map queue 1 threshold 2 1 Switch(config)# mls qos srr-queue input cos-map queue 2 threshold 1 2 Switch(config)# mls qos srr-queue input cos-map queue 2 threshold 2 4 6 7 Switch(config)# mls qos srr-queue input cos-map queue 2 threshold 3 3 5</td>
</tr>
<tr>
<td>The switch automatically maps CoS values to an egress queue in the queue-set and to a threshold ID.</td>
<td>Switch(config)# no mls qos srr-queue output cos-map Switch(config)# mls qos srr-queue output cos-map queue 1 threshold 3 5 Switch(config)# mls qos srr-queue output cos-map queue 2 threshold 3 3 6 7 Switch(config)# mls qos srr-queue output cos-map queue 3 threshold 3 2 4 Switch(config)# mls qos srr-queue output cos-map queue 4 threshold 2 1 Switch(config)# mls qos srr-queue output cos-map queue 4 threshold 3 0</td>
</tr>
<tr>
<td>The switch automatically maps DSCP values to an ingress queue and to a threshold ID.</td>
<td>Switch(config)# no mls qos srr-queue input dscp-map Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 2 9 10 11 12 13 14 15 Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 3 0 1 2 3 4 5 6 7 Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 3 32 Switch(config)# mls qos srr-queue input dscp-map queue 2 threshold 1 16 17 18 19 20 21 22 23 Switch(config)# mls qos srr-queue input dscp-map queue 2 threshold 2 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 Switch(config)# mls qos srr-queue input dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31 Switch(config)# mls qos srr-queue input dscp-map queue 2 threshold 4 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47</td>
</tr>
</tbody>
</table>
### Table 34-6 Generated Auto-QoS Configuration (continued)

<table>
<thead>
<tr>
<th>Description</th>
<th>Automatically Generated Command</th>
</tr>
</thead>
</table>
| The switch automatically maps DSCP values to an egress queue in the queue-set and to a threshold ID. | Switch(config)# no mls qos srr-queue output dscp-map  
Switch(config)# mls qos srr-queue output dscp-map queue 1 threshold 3 40 41 42 43 44 45 46 47  
Switch(config)# mls qos srr-queue output dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31  
Switch(config)# mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51 52 53 54 55  
Switch(config)# mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59 60 61 62 63  
Switch(config)# mls qos srr-queue output dscp-map queue 3 threshold 3 16 17 18 19 20 21 22 23  
Switch(config)# mls qos srr-queue output dscp-map queue 3 threshold 3 32 33 34 35 36 37 38 39  
Switch(config)# mls qos srr-queue output dscp-map queue 4 threshold 1 8  
Switch(config)# mls qos srr-queue output dscp-map queue 4 threshold 2 9 10 11 12 13 14 15  
Switch(config)# mls qos srr-queue output dscp-map queue 4 threshold 3 0 1 2 3 4 5 6 7 |
| The switch automatically sets up the ingress queues, with queue 2 as the priority queue and queue 1 in shared mode. The switch also configures the bandwidth and buffer size for the ingress queues. | Switch(config)# no mls qos srr-queue input priority-queue 1  
Switch(config)# no mls qos srr-queue input priority-queue 2  
Switch(config)# mls qos srr-queue input bandwidth 90 10  
Switch(config)# mls qos srr-queue input threshold 1 8 16  
Switch(config)# mls qos srr-queue input threshold 2 34 66  
Switch(config)# mls qos srr-queue input buffers 67 33 |
| The switch automatically configures the egress queue-set buffer sizes. It configures the bandwidth and the SRR mode (shaped or shared). | Switch(config)# mls qos queue-set output 1 buffers 10 10 26 54  
Switch(config-if)# srr-queue bandwidth shape 10 0 0 0  
Switch(config-if)# srr-queue bandwidth share 10 10 60 20 |
| The switch automatically sets the ingress classification to trust the CoS value received in the packet on a nonrouted port or to trust the DSCP value received in the packet on a routed port. | Switch(config-if)# mls qos trust cos  
Switch(config-if)# mls qos trust dscp |
| If you entered the **auto qos voip cisco-phone** command, the switch automatically enables the trusted boundary feature, which uses the CDP to detect the presence or absence of a Cisco IP Phone. | Switch(config-if)# mls qos trust device cisco-phone |
Configuring Auto-QoS

Effects of Auto-QoS on the Configuration

When auto-QoS is enabled, the switch adds the `auto qos voip` interface configuration command and the generated configuration to the running configuration.

The switch applies the auto-QoS-generated commands as if the commands were entered from the CLI. An existing user configuration can cause the application of the generated commands to fail, or the user configuration might be overridden by the generated commands. These actions occur without warning. If all the generated commands are successfully applied, any user-entered configuration that was not overridden remains in the running configuration. Any user-entered configuration that was overridden can be retrieved by reloading the switch without saving the current configuration to memory. If the generated commands are not applied, the previous running configuration is restored.

Auto-QoS Configuration Guidelines

Before configuring auto-QoS, you should be aware of this information:

- In releases earlier than Cisco IOS Release 12.2(25)EY, auto-QoS configures VOIP only on switch ports with Cisco IP Phones.
- In Cisco IOS Release 12.2(25)EY or later, auto-QoS configures the switch for VoIP with Cisco IP Phones on nonrouted and routed ports. Auto-QoS also configures the switch for VoIP with devices running the Cisco SoftPhone application.

Note

When a device running Cisco SoftPhone is connected to a nonrouted or routed port, the switch supports only one Cisco SoftPhone application per port.
To take advantage of the auto-QoS features, you should enable auto-QoS before you configure other QoS commands. If necessary, you can fine-tune the QoS configuration, but we recommend that you do so only after the auto-QoS configuration is completed. For more information, see the “Effects of Auto-QoS on the Configuration” section on page 34-45.

After auto-QoS is enabled, do not modify a policy map or aggregate policer that includes AutoQoS in its name. If you need to modify the policy map or aggregate policer, make a copy of it, and change the copied policy map or policer. To use this new policy map instead of the generated one, remove the generated policy map from the interface, and apply the new policy map to the interface.

You can enable auto-QoS on static, dynamic-access, voice VLAN access, and trunk ports.

By default, the CDP is enabled on all ports. For auto-QoS to function properly, do not disable the CDP.

When enabling auto-QoS with a Cisco IP Phone on a routed port, you must assign a static IP address to the IP phone.

This release supports only Cisco IP SoftPhone Version 1.3(3) or later.

Connected devices must use Cisco Call Manager Version 4 or later.

You can manually enable policing, as described in the “Configuring an Ingress QoS Policy” section on page 34-63.

Upgrading from a Previous Software Release

In Cisco IOS Release 12.2(25)EY, the implementation for auto-QoS changed from the previous release. The generated auto-QoS configuration was changed, support for the Cisco SoftPhone feature was added, and support for Cisco IP Phones on routed ports was added.

If auto-QoS is configured on the switch, your switch is running a release earlier than Cisco IOS Release 12.2(25)EY, and you upgrade to Cisco IOS Release 12.2(25)EY or later, the configuration file will not contain the new configuration, and auto-QoS will not operate. Follow these steps to update the auto-QoS settings in your configuration file:

1. Upgrade your switch to Cisco IOS Release 12.2(25)EY or later.
2. Disable auto-QoS on all ports on which auto-QoS was enabled.
3. Return all the global auto-QoS settings to their values by using the no commands.
4. Re-enable auto-QoS on the ports on which auto-QoS was disabled in Step 2. Configure the ports with the same auto-QoS settings as the previous ones.

Enabling Auto-QoS for VoIP

Beginning in privileged EXEC mode, follow these steps to enable auto-QoS for VoIP within a QoS domain:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>interface interface-id</td>
<td>Specify the port that is connected to a Cisco IP Phone or the uplink port that is connected to another switch or router in the interior of the network, and enter interface configuration mode.</td>
</tr>
</tbody>
</table>
To display the QoS commands that are automatically generated when auto-QoS is enabled or disabled, enter the **debug autoqos** privileged EXEC command before enabling auto-QoS. For more information, see the “debug autoqos” command in the command reference for this release.

To disable auto-QoS on a port, use the **no auto qos voip** interface configuration command. Only the auto-QoS-generated interface configuration commands for this port are removed. If this is the last port on which auto-QoS is enabled and you enter the **no auto qos voip** command, auto-QoS is considered disabled even though the auto-QoS-generated global configuration commands remain (to avoid disrupting traffic on other ports affected by the global configuration). You can use the **no mls qos** global configuration command to disable the auto-QoS-generated global configuration commands. With QoS disabled, there is no concept of trusted or untrusted ports because the packets are not modified (the CoS, DSCP, and IP precedence values in the packet are not changed). Traffic is switched in pass-through mode (packets are switched without any rewrites and classified as best effort without any policing).

This example shows how to enable auto-QoS on a port and to trust the QoS labels received in inbound packets when the switch or router connected to a port is a trusted device:

```bash
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# auto qos voip trust
```
Auto-QoS Configuration Example

This section describes how you could implement auto-QoS in a network, as shown in Figure 34-13.

*Figure 34-13  Auto-QoS Configuration Example Network*

Figure 34-13 shows a network in which the VoIP traffic is prioritized over all other traffic. Auto-QoS is enabled on the switches in the wiring closets at the edge of the QoS domains.

You should not configure any standard QoS commands before entering the auto-QoS commands. You can fine-tune the QoS configuration, but we recommend that you do so only after the auto-QoS configuration is completed.
Beginning in privileged EXEC mode, follow these steps to configure the switch at the edge of the QoS domain to prioritize the VoIP traffic over all other traffic:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>debug auto qos</code></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>configure terminal</code></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>cdp enable</code></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>interface interface-id</code></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>auto qos voip cisco-phone</code></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>exit</code></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Repeat Steps 4 to 6 for as many ports as are connected to the Cisco IP Phone.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><code>auto qos voip cisco-phone</code></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td><code>exit</code></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td><code>interface interface-id</code></td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td><code>auto qos voip trust</code></td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td><code>end</code></td>
</tr>
<tr>
<td><strong>Step 13</strong></td>
<td><code>show auto qos</code></td>
</tr>
<tr>
<td><strong>Step 14</strong></td>
<td><code>copy running-config startup-config</code></td>
</tr>
</tbody>
</table>

**Displaying Auto-QoS Information**

To display the initial auto-QoS configuration, use the `show auto qos [interface [interface-id]]` privileged EXEC command. To display any user changes to that configuration, use the `show running-config` privileged EXEC command. You can compare the `show auto qos` and the `show running-config` command displays to identify the user-defined QoS settings.
Configuring Standard QoS

Before configuring standard QoS, you must have a thorough understanding of these items:

- The types of applications used and the traffic patterns on your network.
- Traffic characteristics and needs of your network. Is the traffic bursty? Do you need to reserve bandwidth for voice and video streams?
- Bandwidth requirements and speed of the network.
- Location of congestion points in the network.

These sections describe how to configure standard QoS on your switch:

- Standard QoS Configuration, page 34-50
- Standard QoS Configuration Guidelines, page 34-53
- Packet Modification, page 34-55
- Enabling QoS Globally, page 34-56 (required)
- Configuring Ingress Classification by Using Port Trust States, page 34-56 (required)
- Configuring an Ingress QoS Policy, page 34-63 (required)
- Configuring DSCP Maps, page 34-80 (optional, unless you need to use the DSCP-to-DSCP-mutation map or the policed-DSCP map)
- Configuring Ingress Queue Characteristics, page 34-86 (optional)
- Configuring Egress Queue-Set Characteristics, page 34-91 (optional)

If you need to configure outbound traffic on an ES port, see the “Configuring Hierarchical QoS” section on page 34-103.

Standard QoS Configuration

QoS is disabled. There is no concept of trusted or untrusted ports because the packets are not modified (the CoS, DSCP, and IP precedence values in the packet are not changed). Traffic is switched in pass-through mode (packets are switched without any rewrites and classified as best effort without any policing).
When QoS is enabled with the `mls qos` global configuration command and all other QoS settings are at their default values, traffic is classified as best effort (the DSCP and CoS value is set to 0) without any policing. No policy maps are configured. The port trust state on all ports is untrusted. The ingress queues and egress queue-set settings are described in the “Ingress Queue Configuration” section on page 34-51 and the “Egress Queue-Set Configuration” section on page 34-52. For traffic on an ES port, see the “Hierarchical QoS Configuration” section on page 34-103.

**Ingress Queue Configuration**

Single-level input policy maps are supported on standard ports, ES ports, and SVIs. Table 34-7 shows the ingress queue configuration when QoS is enabled.

**Table 34-7  Ingress Queue Configuration**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Queue 1</th>
<th>Queue 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buffer allocation</td>
<td>90 percent</td>
<td>10 percent</td>
</tr>
<tr>
<td>Bandwidth allocation¹</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Priority queue bandwidth²</td>
<td>0</td>
<td>10</td>
</tr>
<tr>
<td>WTD drop threshold 1</td>
<td>100 percent</td>
<td>100 percent</td>
</tr>
<tr>
<td>WTD drop threshold 2</td>
<td>100 percent</td>
<td>100 percent</td>
</tr>
</tbody>
</table>

1. The bandwidth is equally shared between the queues. SRR sends packets in shared mode only.

2. Queue 2 is the priority queue. SRR services the priority queue for its configured share before servicing the other queue.

Table 34-8 shows the CoS input queue threshold map when QoS is enabled.

**Table 34-8  CoS Input Queue Threshold Map**

<table>
<thead>
<tr>
<th>CoS Value</th>
<th>Queue ID–Threshold ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>0–4</td>
<td>1–1</td>
</tr>
<tr>
<td>5</td>
<td>2–1</td>
</tr>
<tr>
<td>6, 7</td>
<td>1–1</td>
</tr>
</tbody>
</table>

Table 34-9 shows the DSCP input queue threshold map when QoS is enabled.

**Table 34-9  DSCP Input Queue Threshold Map**

<table>
<thead>
<tr>
<th>DSCP Value</th>
<th>Queue ID–Threshold ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>0–39</td>
<td>1–1</td>
</tr>
<tr>
<td>40–47</td>
<td>2–1</td>
</tr>
<tr>
<td>48–63</td>
<td>1–1</td>
</tr>
</tbody>
</table>
Egress Queue-Set Configuration

Single-level output policy maps are supported on SVIs and ES ports. Table 34-10 shows the default egress queue-set configuration when QoS is enabled. All ports are mapped to queue-set 1. The port bandwidth limit is set to 100 percent, and the rate is unlimited.

Table 34-10  Egress Queue-Set Configuration

<table>
<thead>
<tr>
<th>Feature</th>
<th>Queue 1</th>
<th>Queue 2</th>
<th>Queue 3</th>
<th>Queue 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buffer allocation</td>
<td>25 percent</td>
<td>25 percent</td>
<td>25 percent</td>
<td>25 percent</td>
</tr>
<tr>
<td>WTD drop threshold 1</td>
<td>100 percent</td>
<td>200 percent</td>
<td>100 percent</td>
<td>100 percent</td>
</tr>
<tr>
<td>WTD drop threshold 2</td>
<td>100 percent</td>
<td>200 percent</td>
<td>100 percent</td>
<td>100 percent</td>
</tr>
<tr>
<td>Reserved threshold</td>
<td>50 percent</td>
<td>50 percent</td>
<td>50 percent</td>
<td>50 percent</td>
</tr>
<tr>
<td>Maximum threshold</td>
<td>400 percent</td>
<td>400 percent</td>
<td>400 percent</td>
<td>400 percent</td>
</tr>
<tr>
<td>SRR shaped weights (absolute)</td>
<td>25</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>SRR shared weights</td>
<td>25</td>
<td>25</td>
<td>25</td>
<td>25</td>
</tr>
</tbody>
</table>

1. A shaped weight of zero means that this queue is operating in shared mode.
2. One quarter of the bandwidth is allocated to each queue.

Table 34-11 shows the CoS output queue threshold map when QoS is enabled.

Table 34-11  CoS Output Queue Threshold Map

<table>
<thead>
<tr>
<th>CoS Value</th>
<th>Queue ID–Threshold ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>0, 1</td>
<td>2–1</td>
</tr>
<tr>
<td>2, 3</td>
<td>3–1</td>
</tr>
<tr>
<td>4</td>
<td>4–1</td>
</tr>
<tr>
<td>5</td>
<td>1–1</td>
</tr>
<tr>
<td>6, 7</td>
<td>4–1</td>
</tr>
</tbody>
</table>

Table 34-12 shows the DSCP output queue threshold map when QoS is enabled.

Table 34-12  DSCP Output Queue Threshold Map

<table>
<thead>
<tr>
<th>DSCP Value</th>
<th>Queue ID–Threshold ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>0–15</td>
<td>2–1</td>
</tr>
<tr>
<td>16–31</td>
<td>3–1</td>
</tr>
<tr>
<td>32–39</td>
<td>4–1</td>
</tr>
<tr>
<td>40–47</td>
<td>1–1</td>
</tr>
<tr>
<td>48–63</td>
<td>4–1</td>
</tr>
</tbody>
</table>
Mapping Table Configuration

The CoS-to-DSCP map is shown in Table 34-13 on page 34-81.
The IP-precedence-to-DSCP map is shown in Table 34-14 on page 34-82.
The DSCP-to-CoS map is shown in Table 34-15 on page 34-84.
The DSCP-to-DSCP-mutation map is a null map, which maps an inbound DSCP value to the same DSCP value.
The policed-DSCP map is a null map, which maps an inbound DSCP value to the same DSCP value (no markdown).

Standard QoS Configuration Guidelines

Before beginning the QoS configuration, you should be aware of this information:

- It is not possible to match IP fragments against configured IP extended ACLs to enforce QoS. IP fragments are sent as best-effort. IP fragments are denoted by fields in the IP header.
- Only one ACL can be configured per class map. The ACL can have multiple ACEs, which match fields against the contents of the packet. Class maps that contain ACLs are supported only in an ingress nonhierarchical single-level policy attached to a standard port or an SVI. You can only use the `match access-group acl-index-or-name` class-map configuration command in a nonhierarchical policy map attached to a standard port, an SVI, or an ES port. For information on hierarchical service policies attached to the ES ports, see the “Configuring Hierarchical QoS” section on page 34-103.
- Only one policy map per port is supported. You can attach one ingress nonhierarchical service policy per standard physical port or per SVI. You can also attach one ingress hierarchical service policy per SVI.
- Inbound traffic is classified, policed, and marked down (if configured) regardless of whether the traffic is bridged, routed, or sent to the CPU. Bridged frames can be dropped or have their DSCP and CoS values modified.
- Only one ingress policer is applied to a packet on a port. Only the average-rate and committed-burst parameters are configurable.
- You can create an aggregate policer that is shared by multiple traffic classes within the same policy map. However, you cannot use the aggregate policer across different policy maps.
- For standard ports and ES ports, the port ASIC device supports a total of 256 policers on the switch. Of these, 255 are user-configurable; one is reserved for internal use. The maximum number of policers that can be configured per port is 63. For example, you could configure 32 policers on a Gigabit Ethernet port and 8 policers on a Fast Ethernet port, or you could configure 63 policers on a Gigabit Ethernet port and 5 policers on a Fast Ethernet port. Policers are allocated on demand by the software and are constrained by the hardware and ASIC boundaries. You cannot reserve policers per port; there is no guarantee that a port will be assigned to any policer. These limitations do not apply to policers configured in a hierarchical policy attached to an ES port.
- On a port configured for QoS, all traffic received through the port is classified, policed, and marked according to the policy map attached to the port. On a trunk port configured for QoS, traffic in all VLANs received through the port is classified, policed, and marked according to the policy map attached to the port.
- On releases earlier than Cisco IOS Release 12.2(35)SE, the switch does not support attaching a standard (one-level) service policy to a logical interface (such as an EtherChannel). If you have EtherChannel ports configured on your switch, you must configure QoS classification, policing,
mapping, and queueing on the individual physical ports that comprise the EtherChannel. Beginning with Cisco IOS Release 12.2(35)SE, the switch supports EtherChannels made of ES ports for single-level output policy maps and hierarchical policy maps in both directions.

- Control traffic (such as spanning-tree bridge protocol data units [BPDUs] and routing update packets) received by the switch are subject to all ingress QoS processing.
- You are likely to lose data when you change queue settings; therefore, try to make changes when traffic is at a minimum.
- Follow these guidelines when the egress priority queue is enabled on a port; otherwise, the egress queues are serviced based on their SRR weights:
  - If the egress priority queue is enabled, it overrides the SRR shaped and shared weights for queue 1.
  - If the egress priority queue is disabled and the SRR shaped and shared weights are configured, the shaped mode overrides the shared mode for queue 1, and SRR services this queue in shaped mode.
  - If the egress priority queue is disabled and the SRR shaped weights are not configured, SRR services this queue in shared mode.
- In Cisco IOS Release 12.2(44)SE or later, if the mls qos global configuration command is disabled and you do not explicitly configure the cpu traffic qos global configuration command, the switch uses the default behavior. The default is no marking for CPU-generated traffic and all packets queued to queue 1.
- In Cisco IOS Release 12.2(25)EY or later, follow these guidelines when configuring policy maps on physical ports or SVIs:
  - You cannot apply the same policy map to a physical port and to an SVI.
  - If VLAN-based QoS is configured on a physical port, the switch removes all the port-based policy maps on the port. The traffic on this physical port is now affected by the policy map attached to the SVI to which the physical port belongs.
  - In a dual-level policy map attached to an SVI, you can only configure an individual policer at the interface level on a physical port to specify the bandwidth limits for the traffic on the port. The ingress port must be configured as a trunk or as a static-access port. You cannot configure policers at the VLAN level of the dual-level policy map.
  - The switch does not support aggregate policers in dual-level policy maps.
  - After the dual-level policy map is attached to an SVI, the interface-level policy map cannot be modified or removed from the dual-level policy map. A new interface-level policy map also cannot be added to the dual-level policy map. You also cannot add or remove a class map specified in the dual-level policy map. If you want these changes to occur, the hierarchical policy map must first be removed from the SVI.

For outbound traffic on an ES port, see the “Hierarchical QoS Configuration Guidelines” section on page 34-103.
Packet Modification

A packet is classified, policed, and queued to provide QoS. Packet modifications can occur during this process:

- For IP and non-IP packets, ingress classification involves assigning a QoS label to a packet based on the DSCP or CoS of the received packet. However, the packet is not modified at this stage; only an indication of the assigned DSCP or CoS value is carried along. The reason for this is that QoS classification and forwarding lookups occur in parallel, and it is possible that the packet is forwarded with its original DSCP to the CPU where it is again processed through software.

When the ES ports classify traffic at egress, this classification can be used for queuing or for marking the CoS, DSCP, IP precedence, or MPLS EXP bits. Any packet modifications that result from ingress classification are applied before the packet reaches the egress classification stage. For example, if the switch receives traffic with a CoS value of 2 and an ingress action resets the CoS to 4, the packet will have a CoS of 4 (instead of a CoS of 2 and an indicator that the CoS should be set to 4) when it moves to the egress classification stage.

- During ingress policing, IP and non-IP packets can have another DSCP assigned to them (if they are out of profile and the policer specifies a markdown DSCP). Once again, the DSCP in the packet is not modified, but an indication of the marked-down value is carried along. For IP packets, the packet modification occurs at a later stage; for non-IP packets the DSCP is converted to CoS and used for queueing and scheduling decisions.

During egress policing on the ES ports, marking actions can set the CoS, DSCP, IP precedence, or the MPLS EXP bits. Any markings performed by an ingress policer are applied before the packet reaches the egress classification stage.

- Depending on the QoS label assigned to a frame and the mutation chosen, the DSCP and CoS values of the frame are rewritten. If you do not configure the mutation map and if you configure the port to trust the DSCP of the inbound frame, the DSCP value in the frame is not changed, but the CoS is rewritten according to the DSCP-to-CoS map. If you configure the port to trust the CoS of the inbound frame and it is an IP packet, the CoS value in the frame is not changed, but the DSCP might be changed according to the CoS-to-DSCP map.

The input mutation causes the DSCP to be rewritten depending on the new value of DSCP chosen. The set action in a policy map also causes the DSCP to be rewritten.

This information applies to both standard and ES ports. On the ES ports, the switch also applies trust policies to IEEE 802.1Q tunneling frames at egress.

- If you apply an ingress hierarchical policy to an ES port, packets can be queued, dropped, and changed because of the marking process that occurs before the standard ingress actions.
Enabling QoS Globally

By default, QoS is disabled on the switch.

Beginning in privileged EXEC mode, follow these steps to enable QoS. This procedure is required.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 mls qos</td>
<td>Enable QoS globally.</td>
</tr>
<tr>
<td>Step 3 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4 show mls qos</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 5 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable QoS, use the **no mls qos** global configuration command.

Configuring Ingress Classification by Using Port Trust States

These sections describe how to classify inbound traffic through port trust states. Depending on your network configuration, you must perform one or more of these tasks or one or more of the tasks in the “Configuring an Ingress QoS Policy” section on page 34-63:

- Configuring the Trust State on Ports Within the QoS Domain, page 34-56
- Configuring the CoS Value for an Interface, page 34-59
- Configuring a Trusted Boundary to Ensure Port Security, page 34-60
- Enabling DSCP Transparency Mode, page 34-61
- Configuring the DSCP Trust State on a Port Bordering Another QoS Domain, page 34-61

Configuring the Trust State on Ports Within the QoS Domain

Packets entering a QoS domain are classified at the edge of the QoS domain. The switch port within the QoS domain can then be configured to one of the trusted states because there is no need to classify the packets at every switch within the domain. Figure 34-14 shows a sample network topology.
Beginning in privileged EXEC mode, follow these steps to configure the port to trust the classification of the traffic that it receives:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Specify the port to be trusted, and enter interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Valid interfaces include physical ports.</td>
</tr>
</tbody>
</table>
Chapter 34 Configuring QoS

Configuring Standard QoS

To return a port to its untrusted state, use the `no mls qos trust` interface configuration command.

For information on how to change the CoS value, see the “Configuring the CoS Value for an Interface” section on page 34-59. For information on how to configure the CoS-to-DSCP map, see the “Configuring the CoS-to-DSCP Map” section on page 34-81.

### Step 3

- **Command**

  - `mls qos trust [cos | dscp | ip-precedence]`

  Configure the port trust state.

  By default, the port is not trusted. If no keyword is specified, the default is `dscp`.

  For 802.1Q tunnels, the switch processes inbound traffic on a standard port according to the trusted setting applied to this port. The switch configures the inner and outer tags for packets sent over the ES trunk port.

  The keywords have these meanings:

  - **cos**—Classifies an ingress packet by using the packet CoS value. For an untagged packet, the port CoS value is used. The port CoS value is 0.

    For IEEE 802.1Q tunnels, the switch copies the inner CoS value to the outer CoS value and sends the packet out an ES port.

  - **dscp**—Classifies an ingress packet by using the packet DSCP value if the packet is an IP packet. For a non-IP packet, the packet CoS value is used if the packet is tagged; for an untagged packet, the port CoS is used.

    Internally, the switch maps the CoS value to a DSCP value by using the CoS-to-DSCP map.

    For IEEE 802.1Q tunnels, for a non-IP packet that is untagged, the switch configures the outer CoS value from the DSCP-to-CoS map, does not modify the inner CoS value, and sends the packet out an ES port. For an IP packet, the switch modifies the DSCP value in the packet if there is a DSCP-to-DSCP mutation map configured on the standard port. The switch uses the mutated DSCP value to configure the outer CoS value from the DSCP-to-CoS map and sends the packet out an ES port.

  - **ip-precedence**—Classifies an ingress packet by using the packet IP-precedence value. For a non-IP packet, the packet CoS value is used if the packet is tagged; for an untagged packet, the port CoS is used.

    Internally, the switch maps the CoS value to a DSCP value through the CoS-to-DSCP map.

    For 802.1Q tunnels, the switch converts the generated DSCP value from the DSCP-to-CoS map and uses it as the outer CoS value in the packet. The switch does not modify the inner CoS value in the packet and sends the packet out an ES port.

  **Note**  When port trust policies are used with IEEE 802.1Q tunneling, all ports sharing the same tunnel VLAN must be configured with the same trust policy, and the ports involved must use the same DSCP-to-DSCP mutation map. For more information, see the “Configuring the DSCP-to-DSCP-Mutation Map” section on page 34-85.

### Step 4

- **Command**

  - `end`

  Return to privileged EXEC mode.

### Step 5

- **Command**

  - `show mls qos interface`

  Verify your entries.

### Step 6

- **Command**

  - `copy running-config startup-config`

  (Optional) Save your entries in the configuration file.
Configuring the CoS Value for an Interface

QoS assigns the CoS value specified with the `mls qos cos` interface configuration command to untagged frames received on trusted and untrusted ports.

Beginning in privileged EXEC mode, follow these steps to define the CoS value of a port or to assign the CoS to all inbound packets on the port:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> interface interface-id</td>
<td>Specify the port to be configured, and enter interface configuration mode. Valid interfaces include physical ports.</td>
</tr>
<tr>
<td><strong>Step 3</strong> mls qos cos {-cos</td>
<td>override}</td>
</tr>
<tr>
<td></td>
<td>• For <code>-cos</code>, specify a CoS value to be assigned to a port. If the packet is untagged, the CoS value becomes the packet CoS value. The CoS range is 0 to 7. The default is 0.</td>
</tr>
<tr>
<td></td>
<td>• Use the <code>override</code> keyword to override the previously configured trust state of the inbound packet and to apply the port CoS value to the port on all inbound packets. By default, CoS override is disabled.</td>
</tr>
<tr>
<td></td>
<td>Use the <code>override</code> keyword when all inbound packets on specified ports deserve higher or lower priority than packets entering from other ports. Even if a port was previously set to trust DSCP, CoS, or IP precedence, this command overrides the previously configured trust state, and all the inbound CoS values are assigned the CoS value configured with this command. If an inbound packet is tagged, the CoS value of the packet is modified with the default CoS of the port at the ingress port.</td>
</tr>
<tr>
<td></td>
<td>When an incoming packet is received on an interface acting as an IEEE 802.1Q tunnel and is sent out an ES port, the switch modifies the outer CoS value and does not modify the inner CoS value.</td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 5</strong> show mls qos interface</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td><strong>Step 6</strong> copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default setting, use the `no mls qos cos {-cos | override}` interface configuration command.
Configuring a Trusted Boundary to Ensure Port Security

In a typical network, you connect a Cisco IP Phone to a switch port, as shown in Figure 34-14 on page 34-57, and cascade devices that generate data packets from the back of the telephone. The Cisco IP Phone guarantees the voice quality through a shared data link by marking the CoS level of the voice packets as high priority (CoS = 5) and by marking the data packets as low priority (CoS = 0). Traffic sent from the telephone to the switch is typically marked with a tag that uses the 802.1Q header. The header contains the VLAN information and the CoS 3-bit field, which is the priority of the packet.

For most Cisco IP Phone configurations, the traffic sent from the telephone to the switch should be trusted to ensure that voice traffic is properly prioritized over other types of traffic in the network. By using the `mls qos trust cos` interface configuration command, you configure the switch port to which the telephone is connected to trust the CoS labels of all traffic received on that port.

With the trusted setting, you also can use the trusted boundary feature to prevent misuse of a high-priority queue if a user bypasses the telephone and connects the PC directly to the switch. Without trusted boundary, the CoS labels generated by the PC are trusted by the switch (because of the trusted CoS setting). By contrast, trusted boundary uses CDP to detect the presence of a Cisco IP Phone (such as the Cisco IP Phone 7910, 7935, 7940, and 7960) on a switch port. If the telephone is not detected, the trusted boundary feature disables the trusted setting on the switch port and prevents misuse of a high-priority queue. Note that the trusted boundary feature is not effective if the PC and Cisco IP Phone are connected to a hub that is connected to the switch.

In some situations, you can prevent a PC connected to the IP phone from taking advantage of a high-priority data queue. You can use the `switchport priority extend cos` interface configuration command to configure the telephone through the switch CLI to override the priority of the traffic received from the PC.

Beginning in privileged EXEC mode, follow these steps to enable trusted boundary on a port:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>cdp run</td>
</tr>
<tr>
<td>Step 3</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 4</td>
<td>cdp enable</td>
</tr>
<tr>
<td>Step 5</td>
<td>mls qos trust cos</td>
</tr>
<tr>
<td>Step 6</td>
<td>mls qos trust device cisco-phone</td>
</tr>
<tr>
<td>Step 7</td>
<td>end</td>
</tr>
<tr>
<td>Step 8</td>
<td>show mls qos interface</td>
</tr>
<tr>
<td>Step 9</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To disable the trusted boundary feature, use the `no mls qos trust device` interface configuration command.
Enabling DSCP Transparency Mode

In software releases earlier than Cisco IOS Release 12.1(14)AX2, if QoS is disabled, the DSCP value of the incoming IP packet is not modified. If QoS is enabled and you configure the interface to trust DSCP, the switch does not modify the DSCP value. If you configure the interface to trust CoS, the switch modifies the DSCP value according to the CoS-to-DSCP map.

In Cisco IOS Release 12.1(14)AX2 or later, the switch supports the DSCP transparency feature. It affects only the DSCP field of a packet at egress. By default, DSCP transparency is disabled. The switch modifies the DSCP field in an incoming packet, and the DSCP field in the outgoing packet is based on the quality of service (QoS) configuration, including the port trust setting, policing and marking, and the DSCP-to-DSCP mutation map.

If DSCP transparency is enabled by using the `no mls qos rewrite ip dscp` command, the switch does not modify the DSCP field in the incoming packet, and the DSCP field in the outgoing packet is the same as that in the incoming packet.

Regardless of the DSCP transparency configuration, the switch modifies the internal DSCP value of the packet, which the switch uses to generate a class of service (CoS) value that represents the priority of the traffic. The switch also uses the internal DSCP value to select an egress queue and threshold.

On an ES port, if an action in an egress policy map modifies the DSCP value of the packet and the policy map is applied to the ES port, the switch modifies the DSCP value regardless of the DSCP transparency configuration.

Beginning in privileged EXEC mode, follow these steps to enable DSCP transparency on a switch:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>mls qos</td>
<td>Enable QoS globally.</td>
</tr>
<tr>
<td>3</td>
<td>no mls qos rewrite ip dscp</td>
<td>Enable DSCP transparency. The switch is configured to not modify the DSCP field of the IP packet.</td>
</tr>
<tr>
<td>4</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>5</td>
<td>show mls qos interface [interface-id]</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>6</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To configure the switch to modify the DSCP value based on the trust setting or on an ACL by disabling DSCP transparency, use the `mls qos rewrite ip dscp` global configuration command.

If you disable QoS by using the `no mls qos` global configuration command, the CoS and DSCP values are not changed (the default QoS setting).

If you enter the `no mls qos rewrite ip dscp` global configuration command to enable DSCP transparency and then enter the `mls qos trust [cos | dscp]` interface configuration command, DSCP transparency is still enabled.

Configuring the DSCP Trust State on a Port Bordering Another QoS Domain

If you are administering two separate QoS domains between which you want to implement QoS features for IP traffic, you can configure the switch ports bordering the domains to a DSCP-trusted state as shown in Figure 34-15. Then the receiving port accepts the DSCP-trusted value and avoids the classification...
stage of QoS. If the two domains use different DSCP values, you can configure the DSCP-to-DSCP-mutation map to translate a set of DSCP values to match the definition in the other domain.

**Figure 34-15 DSCP-Trusted State on a Port Bordering Another QoS Domain**

Beginning in privileged EXEC mode, follow these steps to configure the DSCP-trusted state on a port and modify the DSCP-to-DSCP-mutation map. To ensure a consistent mapping strategy across both QoS domains, you must perform this procedure on the ports in both domains:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
</tbody>
</table>
| **Step 2** mls qos map dscp-mutation  
dscp-mutation-name in-dscp to out-dscp | Modify the DSCP-to-DSCP-mutation map.  
The DSCP-to-DSCP-mutation map is a null map, which maps an inbound DSCP value to the same DSCP value.  
- For `dscp-mutation-name`, enter the mutation map name. You can create more than one map by specifying a new name.  
- For `in-dscp`, enter up to eight DSCP values separated by spaces.  
  Then enter the `to` keyword.  
- For `out-dscp`, enter a single DSCP value.  
The DSCP range is 0 to 63. |
| **Step 3** interface interface-id | Specify the port to be trusted, and enter interface configuration mode.  
Valid interfaces include physical ports. |
| **Step 4** mls qos trust dscp | Configure the ingress port as a DSCP-trusted port. By default, the port is not trusted. |
| **Step 5** mls qos dscp-mutation  
dscp-mutation-name | Apply the map to the specified ingress DSCP-trusted port.  
For `dscp-mutation-name`, specify the mutation map name created in Step 2.  
You can configure multiple DSCP-to-DSCP-mutation maps on an ingress port. |
| **Step 6** end | Return to privileged EXEC mode. |
Configuring Standard QoS

To return a port to its nontrusted state, use the `no mls qos trust` interface configuration command. To return to the default DSCP-to-DSCP-mutation map values, use the `no mls qos map dscp-mutation dscp-mutation-name` global configuration command.

This example shows how to configure a port to the DSCP-trusted state and to modify the DSCP-to-DSCP-mutation map (named `gi1/1/1-mutation`) so that inbound DSCP values 10 to 13 are mapped to DSCP 30:

```
Switch(config)# mls qos map dscp-mutation gi1/1/1-mutation 10 11 12 13 to 30
Switch(config)# interface gigabitethernet1/1/1
Switch(config-if)# mls qos trust dscp
Switch(config-if)# mls qos dscp-mutation gi1/1/1-mutation
Switch(config-if)# end
```

Configuring an Ingress QoS Policy

Configuring an ingress QoS policy typically requires classifying traffic into classes, configuring policies applied to those traffic classes, and attaching the policies to a port.

For background information, see the “Ingress Classification” section on page 34-9 and the “Ingress Policing and Marking” section on page 34-13. For configuration guidelines, see the “Standard QoS Configuration Guidelines” section on page 34-53.

These sections describe how to classify, police, and mark inbound traffic. Depending on your network configuration, you must perform one or more of these tasks:

- Classifying Ingress Traffic by Using ACLs, page 34-63
- Classifying Ingress Traffic by Using Class Maps, page 34-67
- Classifying, Policing, and Marking Ingress Traffic by Using Aggregate Policers, page 34-79

For information on configuring policies for the ES ports, see the “Configuring a Hierarchical QoS Policy” section on page 34-107. This section describes how to classify traffic by using class maps, how to configure a two-rate traffic policer, how to configure class-based packet marking in a traffic policy, how to configure CBWFQ, tail drop, DSCP-based WRED, and IP precedence-based WRED, how to enable LLQ, and how to configure shaping.

Classifying Ingress Traffic by Using ACLs

You can classify ingress IP traffic by using IP standard or IP extended ACLs. You also can classify ingress non-IP traffic by using Layer 2 MAC ACLs.
Beginning in privileged EXEC mode, follow these steps to create an IP standard ACL for inbound IP traffic:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>access-list access-list-number {deny</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>When creating an access list, remember that, by default, the end of the access list contains an implicit deny statement for everything if it did not find a match before reaching the end.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>show access-lists</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To delete an access list, use the **no access-list access-list-number** global configuration command.

This example shows how to allow access for only those hosts on the three specified networks. The wildcard bits apply to the host portions of the network addresses. Any host with a source address that does not match the access list statements is rejected.

```
Switch(config)# access-list 1 permit 192.5.255.0 0.0.0.255
Switch(config)# access-list 1 permit 128.88.0.0 0.0.255.255
Switch(config)# access-list 1 permit 36.0.0.0 0.0.0.255
! (Note: all other access implicitly denied)
```
Beginning in privileged EXEC mode, follow these steps to create an IP extended ACL for inbound IP traffic:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>`access-list access-list-number [deny</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>end</code></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>show access-lists</code></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>copy running-config startup-config</code></td>
</tr>
</tbody>
</table>

To delete an access list, use the **no access-list access-list-number** global configuration command.

This example shows how to create an ACL that permits IP traffic from any source to any destination that has the DSCP value set to 32:

```
Switch(config)# access-list 100 permit ip any any dscp 32
```

This example shows how to create an ACL that permits IP traffic from a source host at 10.1.1.1 to a destination host at 10.1.1.2 with a precedence value of 5:

```
Switch(config)# access-list 100 permit ip host 10.1.1.1 host 10.1.1.2 precedence 5
```
This example shows how to create an ACL that permits PIM traffic from any source to a destination group address of 224.0.0.2 with a DSCP set to 32:

```
Switch(config)# access-list 102 permit pim any 224.0.0.2 dscp 32
```

Beginning in privileged EXEC mode, follow these steps to create a Layer 2 MAC ACL for inbound non-IP traffic:

**Command** | **Purpose**
---|---
**Step 1** | configure terminal
Enter global configuration mode.

**Step 2** | mac access-list extended name
Create a Layer 2 MAC ACL by specifying the name of the list. When you enter this command, the mode changes to extended MAC ACL configuration.

**Step 3** | `permit | deny` `host` `src-MAC-addr mask` | `any` `host` `dst-MAC-addr` `mask` | `type` `mask`
Specify the type of traffic to permit or deny if the conditions are matched, entering the command as many times as necessary.
- For `src-MAC-addr`, enter the MAC address of the host from which the packet is being sent. You specify this by using the hexadecimal format (H.H.H), by using the `any` keyword as an abbreviation for `source 0.0.0`, `source-wildcard` `ffff.ffff.ffff`, or by using the `host` keyword for `source 0.0.0`.
- For `mask`, enter the wildcard bits by placing ones in the bit positions that you want to ignore.
- For `dst-MAC-addr`, enter the MAC address of the host to which the packet is being sent. You specify this by using the hexadecimal format (H.H.H), by using the `any` keyword as an abbreviation for `source 0.0.0`, `source-wildcard` `ffff.ffff.ffff`, or by using the `host` keyword for `source 0.0.0`.
- (Optional) For `type mask`, specify the Ethertype number of a packet with Ethernet II or SNAP encapsulation to identify the protocol of the packet. For `type`, the range is from 0 to 65535, typically specified in hexadecimal. For `mask`, enter the `don’t care` bits applied to the Ethertype before testing for a match.

**Note** | When creating an access list, remember that, by default, the end of the access list contains an implicit deny statement for everything if it did not find a match before reaching the end.

**Step 4** | end
Return to privileged EXEC mode.

**Step 5** | show access-lists
`[access-list-number | access-list-name]`
Verify your entries.

**Step 6** | copy running-config startup-config
(Optional) Save your entries in the configuration file.

To delete an access list, use the `no mac access-list extended access-list-name` global configuration command.

This example shows how to create a Layer 2 MAC ACL with two permit statements. The first statement allows traffic from the host with MAC address 0001.0000.0001 to the host with MAC address 0002.0000.0001. The second statement allows only Ethertype XNS-IDP traffic from the host with MAC address 0001.0000.0002 to the host with MAC address 0002.0000.0002.

```
Switch(config)# mac access-list extended maclist1
Switch(config-ext-macl)# permit 0001.0000.0001 0.0.0 0002.0000.0001 0.0.0
Switch(config-ext-macl)# permit 0001.0000.0002 0.0.0 0002.0000.0002 0.0.0 xns-idp
! (Note: all other access implicitly denied)
```
Classifying Ingress Traffic by Using Class Maps

You use the `class-map` global configuration command to create a class map for matching packets to the class whose name you specify. The class map isolates a specific ingress traffic flow (class) from all other traffic by defining the criteria to use to match against a specific flow. A match criterion is defined with a match statement entered within the class-map configuration mode. Packets are compared to the match criteria configured for a class map. If a packet matches the specified criteria, the packet is considered a member of the class and is forwarded according to the QoS specifications set in the traffic policy.

For information on how to classify traffic on an ES port, see the “Classifying Traffic by Using Hierarchical Class Maps” section on page 34-108.

Beginning in privileged EXEC mode, follow these steps to create a class map and to define the match criterion to classify inbound traffic:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> access-list access-list-number {deny</td>
<td>permit} source [source-wildcard] or access-list access-list-number {deny</td>
</tr>
<tr>
<td><strong>Step 3</strong> class-map [match-all</td>
<td>match-any] class-map-name</td>
</tr>
</tbody>
</table>
### Configuring Standard QoS

#### Configuring QoS

**Step 4**

```plaintext
match { access-group acl-index-or-name \n     ip dscp dscp-list | ip precedence \n     ip-precedence-list }
```

**Purpose**

Define the match criterion to classify traffic.

By default, no match criterion is defined.

Only one ACL per class map is supported.

- For `access-group acl-index-or-name`, specify the number or name of the ACL created in Step 2.
- For `ip dscp dscp-list`, enter a list of up to eight IP DSCP values to match against inbound packets. Separate each value with a space. The range is 0 to 63.
- For `ip precedence ip-precedence-list`, enter a list of up to eight IP-precedence values to match against inbound packets. Separate each value with a space. The range is 0 to 7.

**Step 5**

```plaintext
end
```

**Purpose**

Return to privileged EXEC mode.

**Step 6**

```plaintext
show class-map
```

**Purpose**

Verify your entries.

**Step 7**

```plaintext
copy running-config startup-config
```

(Optional) Save your entries in the configuration file.

To delete an existing class map, use the `no class-map [match-all | match-any] class-map-name` global configuration command. To remove a match criterion, use the `no match { access-group acl-index-or-name | ip dscp | ip precedence }` class-map configuration command.

This example shows how to configure the class map called `class1`. The `class1` has one match criterion, which is access list 103. It permits traffic from any host to any destination that matches a DSCP value of 10.

```plaintext
Switch(config)# access-list 103 permit ip any any dscp 10
Switch(config)# class-map class1
Switch(config-cmap)# match access-group 103
Switch(config-cmap)# exit
```

This example shows how to create a class map called `class2`, which matches inbound traffic with DSCP values of 10, 11, and 12:

```plaintext
Switch(config)# class-map class2
Switch(config-cmap)# match ip dscp 10 11 12
Switch(config-cmap)# exit
```

This example shows how to create a class map called `class3`, which matches inbound traffic with IP-precedence values of 5, 6, and 7:

```plaintext
Switch(config)# class-map class3
Switch(config-cmap)# match ip precedence 5 6 7
Switch(config-cmap)# exit
```

### Marking and Queuing CPU-Generated Traffic

You can mark and queue the control plane traffic that the CPU generates by entering the `cpu traffic qos [cos value | dscp value | precedence value]` and `mls qos srr-queue output cpu queue id threshold id` global configuration commands. You can use these commands to mark a CPU-generated control plane packet with a value and to map the traffic to any of the four egress queues.

Use the `cpu traffic qos` global configuration command to mark the control plane traffic with a CoS, DSCP, or IP precedence value. When you configure the `cpu traffic qos` marking for Ethernet or IP traffic, the control plane traffic that the CPU generates is marked with the values that you specify.
control-plane traffic is marked with these values except for Connectivity Fault Management (CFM) traffic. Cisco IOS IP Service Level Agreements (SLAs) traffic that uses the CFM layer for transacting the messages is not affected. However, IP SLAs traffic that uses UDP or other networking layer protocols is affected by this feature.

To use the `cpu traffic qos` feature, you must globally enable the `mls qos global` configuration command on the switch. You can also mark native VLAN traffic and tag it by entering the `vlan dot1q tag native` global configuration command.

Use the `mls qos srr-queue output cpu-queue` global configuration command to specify an egress queue and a threshold value for CPU-generated traffic. The default egress queue value is 2. You can assign each packet that flows through the switch to a queue and to a threshold. Specifically, you map DSCP or CoS values to an egress queue-set and map DSCP or CoS values to a threshold ID. You use the `mls qos srr-queue output dscp-map queue queue-id {dscp1...dscp8 | threshold threshold-id dscp1...dscp8}` or the `mls qos srr-queue output cos-map queue queue-id {cos1...cos8 | threshold threshold-id cos1...cos8}` global configuration command.

### Classifying, Policing, and Marking Ingress Traffic by Using Nonhierarchical Single-Level Policy Maps

On a physical port, a nonhierarchical single-level policy map specifies which inbound traffic class to act on. You can specify which CoS, DSCP, or IP precedence values in the traffic class to trust. You can specify which DSCP or IP precedence values in the traffic class to set. You can specify the traffic bandwidth limitations for each matched traffic class (policer) and the action to take when the traffic is out of profile (marking).

A policy map also has these characteristics:

- A policy map can contain multiple class statements, each with different match criteria and policers.
- A policy map can contain a predefined default traffic class explicitly placed at the end of the map.
- A separate policy-map class can exist for each type of traffic received through a port.
- A policy-map trust state and a port trust state are mutually exclusive. The last one configured takes effect.

Follow these guidelines when configuring single-level policy maps:

- You can attach only one policy map per ingress port.
- If you configure the IP-precedence-to-DSCP map by using the `mls qos map ip-prec-dscp dscp1...dscp8` global configuration command, the settings only affect packets on ingress interfaces that are configured to trust the IP precedence value. In a policy map, if you set the packet IP precedence value to a new value by using the `set precedence new-precedence` policy-map class configuration command, the egress DSCP value is not affected by the IP-precedence-to-DSCP map. If you want the egress DSCP value to be different than the ingress value, use the `set dscp new-dscp` policy-map class configuration command.

- When you configure a default traffic class by using the `class class-default` policy-map configuration command, unclassified traffic (traffic that does not meet the match criteria specified in the traffic classes) is treated as the default traffic class (class-default).

Before beginning this procedure, make sure that you have created the class map to isolate traffic. For more information, see the “Classifying Ingress Traffic by Using ACLs” section on page 34-63 and the “Classifying Ingress Traffic by Using Class Maps” section on page 34-67.

For information about configuring a policy map for an ES port, see the “Configuring a Hierarchical Two-Rate Traffic Policer” section on page 34-110 and the “Configuring Class-Based Packet Marking in a Hierarchical Traffic Policy” section on page 34-114.
Beginning in privileged EXEC mode, follow these steps to create an ingress single-level policy map:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> policy-map policy-map-name</td>
<td>Create a policy map by entering the policy-map name, and enter policy-map configuration mode. By default, no policy maps are defined. The behavior of a policy map is to set the DSCP to 0 if the packet is an IP packet and to set the CoS to 0 if the packet is tagged. No policing is performed.</td>
</tr>
<tr>
<td><strong>Step 3</strong> class [class-map-name</td>
<td>Defines a traffic classification, and enter policy-map class configuration mode. By default, no policy map class-maps are defined. If a traffic class has already been defined by using the class-map global configuration command, specify its name for class-map-name in this command. A class-default traffic class is pre-defined and can be added to any policy. It is always placed at the end of a policy map. With an implied match any included in the class-default class, all packets that have not already matched the other traffic classes will match class-default.</td>
</tr>
<tr>
<td><strong>Step 4</strong> trust [cos</td>
<td>Configure the trust state, which QoS uses to generate a CoS-based or DSCP-based QoS label. By default, the port is not trusted. If no keyword is specified when the command is entered, the default is dscp. The keywords have these meanings:</td>
</tr>
<tr>
<td><strong>cos</strong>—QoS derives the DSCP value by using the received or port CoS value and the CoS-to-DSCP map.</td>
<td></td>
</tr>
<tr>
<td><strong>dscp</strong>—QoS derives the DSCP value by using the DSCP value from the ingress packet. For non-IP packets that are tagged, QoS derives the DSCP value by using the received CoS value; for non-IP packets that are untagged, QoS derives the DSCP value by using the port CoS value. In either case, the DSCP value is derived from the CoS-to-DSCP map.</td>
<td></td>
</tr>
<tr>
<td><strong>ip-precedence</strong>—QoS derives the DSCP value by using the IP precedence value from the ingress packet and the IP-precedence-to-DSCP map. For non-IP packets that are tagged, QoS derives the DSCP value by using the received CoS value; for non-IP packets that are untagged, QoS derives the DSCP value by using the port CoS value. In either case, the DSCP value is derived from the CoS-to-DSCP map.</td>
<td></td>
</tr>
</tbody>
</table>

For more information, see the “Configuring the CoS-to-DSCP Map” section on page 34-81.
### Step 5

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| `set {dscp new-dscp | precedence new-precedence}` | Mark IP traffic by setting a new value in the packet:  
- For `dscp new-dscp`, enter a new DSCP value to be assigned to the classified traffic. The range is 0 to 63.  
- For `precedence new-precedence`, enter a new IP-precedence value to be assigned to the classified traffic. The range is 0 to 7.  

#### Note
The `set dscp new-dscp` and the `set precedence new-precedence` commands are the same as the `set ip dscp new-dscp` and the `set ip precedence new-precedence` commands. |

### Step 6

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| `police rate-bps burst-byte [exceed-action {drop | policed-dscp-transmit}]` | Define a policer for the classified traffic.  
By default, no policer is defined. For information on the number of policers supported, see the “Standard QoS Configuration Guidelines” section on page 34-53.  
- For `rate-bps`, specify average traffic rate in bps. The range is 8000 to 1000000000.  
- For `burst-byte`, specify the normal burst size in bytes. The range is 8000 to 1000000.  
- (Optional) Specify the action to take when the rates are exceeded. Use the `exceed-action drop` keywords to drop the packet. Use the `exceed-action policed-dscp-transmit` keywords to mark down the DSCP value (through the policed-DSCP map) and send the packet. For more information, see the “Configuring the Policed-DSCP Map” section on page 34-83. |

### Step 7

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>exit</code></td>
<td>Return to policy-map configuration mode.</td>
</tr>
</tbody>
</table>

### Step 8

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>exit</code></td>
<td>Return to global configuration mode.</td>
</tr>
</tbody>
</table>

### Step 9

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| `interface interface-id` | Specify the port to attach to the policy map, and enter interface configuration mode.  
Valid interfaces include physical ports. |

### Step 10

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>service-policy input policy-map-name</code></td>
<td>Specify the ingress policy-map name, and apply it to a port.</td>
</tr>
</tbody>
</table>

### Step 11

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

### Step 12

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show policy-map [policy-map-name [class class-map-name]]</code></td>
<td>Verify your entries.</td>
</tr>
</tbody>
</table>

### Step 13

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To delete an existing policy map, use the `no policy-map policy-map-name` global configuration command. To delete an existing class, use the `no class class-name` policy-map configuration command. To return to the default untrusted state, use the `no trust` policy-map class configuration command. To remove an assigned DSCP or IP precedence value, use the `no set {dscp new-dscp | precedence new-precedence}` policy-map class configuration command. To remove an existing policer, use the `no police rate-bps burst-byte [exceed-action {drop | policed-dscp-transmit}]` policy-map class configuration command. To remove the policy map and interface association, use the `no service-policy input policy-map-name` interface configuration command.
This example shows how to create an ingress policy map and attach it to a port. In the configuration, the IP standard ACL permits traffic from network 10.1.0.0. For traffic matching this classification, the DSCP value in the inbound packet is trusted. If the matched traffic exceeds an average traffic rate of 48000 bps and a normal burst size of 8000 bytes, its DSCP is marked down (based on the policed-DSCP map) and sent.

```
Switch(config)# access-list 1 permit 10.1.0.0 0.0.255.255
Switch(config)# class-map ipclass1
Switch(config-cmap)# match access-group 1
Switch(config-cmap)# exit
Switch(config)# policy-map flow1t
Switch(config-pmap)# class ipclass1
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police 48000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# service-policy input flow1t
```

This example shows how to create a Layer 2 MAC ACL with two permit statements and attach it to a port. The first permit statement allows traffic from the host with MAC address 0001.0000.0001 destined for the host with MAC address 0002.0000.0001. The second permit statement allows only Ethertype XNS-IDP traffic from the host with MAC address 0001.0000.0002 destined for the host with MAC address 0002.0000.0002.

```
Switch(config)# mac access-list extended maclist1
Switch(config-ext-mac)# permit 0001.0000.0001 0.0.0 0002.0000.0001 0.0.0 xns-idp
Switch(config-ext-mac)# exit
Switch(config)# mac access-list extended maclist2
Switch(config-ext-mac)# permit 0001.0000.0003 0.0.0 0002.0000.0003 0.0.0 aarp
Switch(config-ext-mac)# exit
Switch(config)# class-map macclass1
Switch(config-cmap)# match access-group maclist1
Switch(config-cmap)# exit
Switch(config)# policy-map macpolicy1
Switch(config-pmap)# class macclass1
Switch(config-pmap-c)# set dscp 63
Switch(config-pmap-c)# exit
Switch(config)# policy-map macpolicy2
Switch(config-pmap-c)# class macclass2 maclist2
Switch(config-pmap-c)# set dscp 45
Switch(config-pmap-c)# exit
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# mls qos trust cos
Switch(config-if)# service-policy input macpolicy1
```

This example shows how to create a class map that applies to both IPv4 and IPv6 traffic with the default class applied to unclassified traffic:

```
Switch(config)# ip access-list 101 permit ip any any
Switch(config)# ipv6 access-list 105 permit ipv6 any any
Switch(config)# class-map cm-1
Switch(config-cmap)# match access-group 101
Switch(config-cmap)# exit
Switch(config)# class-map cm-2
Switch(config-cmap)# match access-group name ipv6-any
Switch(config-cmap)# exit
Switch(config)# policy-map pm1
Switch(config-pmap)# class cm-1
Switch(config-pmap-c)# set dscp 4
Switch(config-pmap-c)# exit
```
Configuring Standard QoS

Switch(config-pmap)# class cm-2
Switch(config-pmap-c)# set dscp 6
Switch(config-pmap-c)# exit
Switch(config-pmap)# class-class-default
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface G0/1
Switch(config-if)# switch mode access
Switch(config-if)# service-policy input pm1

Classifying, Policing, and Marking Traffic by Using Hierarchical Dual-Level Policy Maps

In Cisco IOS Release 12.2(25)EY or later, you can configure hierarchical dual-level policy maps on SVIs, but not on other types of interfaces. Dual-level policing combines the VLAN- and interface-level policy maps to create a single policy map. For more information, see the “Hierarchical Dual-Level Policing on SVIs” section on page 34-15.

On an SVI, the VLAN-level policy map specifies which traffic class to act on. Actions can include trusting the CoS, DSCP, or IP precedence values or setting a specific DSCP or IP precedence value in the traffic class. Use the interface-level policy map to specify the physical ports that are affected by individual policers.

Follow these guidelines when configuring hierarchical dual-level policy maps:

- Before configuring a dual-level policy map, you must enable VLAN-based QoS on the physical ports that are to be specified at the interface level of the policy map.
- You can attach only one policy map per ingress port or SVI.
- A policy map can contain multiple class statements, each with different match criteria and actions.
- A separate policy-map class can exist for each type of traffic received on the SVI.
- A policy map can contain a predefined default traffic class explicitly placed at the end of the map.
- A policy-map trust state and a port trust state are mutually exclusive, and whichever is configured last takes effect.
- If you configure the IP-precedence-to-DSCP map by using the `mls qos map ip-prec-dscp dscp1...dscp8` global configuration command, the settings only affect packets on ingress interfaces that are configured to trust the IP precedence value. In a policy map, if you set the packet IP precedence value to a new value by using the `set precedence new-precedence` policy-map class configuration command, the egress DSCP value is not affected by the IP-precedence-to-DSCP map. If you want the egress DSCP value to be different from the ingress value, use the `set dscp new-dscp` policy-map class configuration command.
- If VLAN-based QoS is enabled, the dual-level policy map supersedes the previously configured port-based policy map.
- The dual-level policy map is attached to the SVI and affects all traffic belonging to the VLAN. The individual policer in the interface-level traffic classification only affects the traffic on the physical ports specified in that classification. The actions specified in the VLAN-level policy map affects the traffic belonging to the SVI.
- When configuring a dual-level policy map on trunk ports, the VLAN ranges must not overlap. If the ranges overlap, the actions specified in the policy map affect the incoming and outgoing traffic on the overlapped VLANs, and the policy map is not applied properly at ingress and egress.
- Aggregate policers are not supported in dual-level policy maps.
- When VLAN-based QoS is enabled, the switch supports VLAN-based features, such as the VLAN map.
- You can configure a dual-level policy map only on the primary VLAN of a private VLAN.

Beginning in privileged EXEC mode, follow these steps to create a hierarchical dual-level policy map:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
</tr>
<tr>
<td>Step 2</td>
<td>`class-map [match-all</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>`match {access-group acl-index-or-name</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>exit</code></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>exit</code></td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
</tr>
<tr>
<td>6</td>
<td>class-map [match-all</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>match input-interface interface-id-list</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>exit</td>
</tr>
<tr>
<td>9</td>
<td>exit</td>
</tr>
<tr>
<td>10</td>
<td>policy-map policy-map-name</td>
</tr>
<tr>
<td>11</td>
<td>class [class-map-name</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Command and Purpose

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 12     | `police rate-bps burst-byte [exceed-action [drop | Define an individual policer for the classified traffic. By default, no policer is defined. For information on the number of policers supported, see the “Standard QoS Configuration Guidelines” section on page 34-53.  

- For `rate-bps`, specify average traffic rate in bits per second (bps). The range is 8000 to 1000000000.  
  - For `burst-byte`, specify the normal burst size in bytes. The range is 8000 to 1000000.  
  - (Optional) Specify the action to take when the rates are exceeded. Use the `exceed-action drop` keywords to drop the packet. Use the `exceed-action policed-dscp-transmit` keywords to mark down the DSCP value (by using the policed-DSCP map) and send the packet. For more information, see the “Configuring the Policed-DSCP Map” section on page 34-83.  

| 13     | `exit`                                       | Return to policy-map configuration mode.                                                                                                                                                                                                                                                                                    |
| 14     | `exit`                                       | Return to global configuration mode.                                                                                                                                                                                                                                                                                    |
| 15     | `policy-map policy-map-name`                 | Create a VLAN-level policy map by entering the policy-map name, and enter policy-map configuration mode. By default, no policy maps are defined. The behavior of a policy map is to set the DSCP to 0 if the packet is an IP packet and to set the CoS to 0 if the packet is tagged. No policing is performed.  

| 16     | `class class-map-name`                      | Define a VLAN-level traffic classification, and enter policy-map class configuration mode. By default, no policy-map class-maps are defined. If a traffic class has already been defined by using the `class-map` global configuration command, specify its name for `class-map-name` in this command. |
# Chapter 34 Configuring QoS

## Configuring Standard QoS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 17   | `trust [cos | dscp | ip-precedence]` | Configure the trust state, which QoS uses to generate a CoS-based or DSCP-based QoS label.  

**Note** This command is mutually exclusive with the `set` command within the same policy map. If you enter the `trust` command, omit Step 18.  

By default, the port is not trusted. If no keyword is specified when the command is entered, the default is `dscp`.  

The keywords have these meanings:  

- **cos**—QoS derives the DSCP value by using the received or default port CoS value and the CoS-to-DSCP map.  
- **dscp**—QoS derives the DSCP value by using the DSCP value from the ingress packet. For non-IP packets that are tagged, QoS derives the DSCP value by using the received CoS value; for non-IP packets that are untagged, QoS derives the DSCP value by using the port CoS value. In either case, the DSCP value is derived from the CoS-to-DSCP map.  
- **ip-precedence**—QoS derives the DSCP value by using the IP precedence value from the ingress packet and the IP-precedence-to-DSCP map. For non-IP packets that are tagged, QoS derives the DSCP value by using the received CoS value; for non-IP packets that are untagged, QoS derives the DSCP value by using the port CoS value. In either case, the DSCP value is derived from the CoS-to-DSCP map.  

For more information, see the “Configuring the CoS-to-DSCP Map” section on page 34-81. |
| 18   | `set {dscp new-dscp | precedence new-precedence]` | Classify IP traffic by setting a new value in the packet.  

- For `dscp new-dscp`, enter a new DSCP value to be assigned to the classified traffic. The range is 0 to 63.  
- For `precedence new-precedence`, enter a new IP-precedence value to be assigned to the classified traffic. The range is 0 to 7. |
| 19   | `service-policy policy-map-name` | Specify the interface-level policy-map name (from Step 10), and associate it with the VLAN-level policy map.  

If the VLAN-level policy map specifies more than one class, all classes must include the same `service-policy policy-map-name` command. |
| 20   | `exit` | Return to policy-map configuration mode. |
| 21   | `exit` | Return to global configuration mode. |
| 22   | `interface interface-id` | Specify the SVI to which to attach the dual-level policy map, and enter interface configuration mode. |
To delete an existing policy map, use the `no policy-map policy-map-name` command. To delete an existing class map, use the `no class class-map-name` command.

To return to the default untrusted state in a policy map, use the `no trust policy-map configuration` command. To remove an assigned DSCP or IP precedence value, use the `no set {dscp new-dscp | ip precedence new-precedence}` command.

To remove an existing policer in an interface-level policy map, use the `no police rate-bps burst-byte [exceed-action {drop | policed-dscp-transmit}]` command. To remove the dual-level policy map and port associations, use the `no service-policy input policy-map-name` interface configuration command.

This example shows how to create a hierarchical dual-level policy map and attach it to an SVI:

```bash
Switch(config)# access-list 101 permit ip any any
Switch(config)# class-map match-all cm-1
Switch(config-cmap)# match access-group 101
Switch(config-cmap)# exit
Switch(config)# class-map match-all cm-interface-1
Switch(config-cmap)# match input-interface gigabitethernet1/0/1 gigabitethernet1/0/2
Switch(config-cmap)# exit
Switch(config)# policy-map port-plcm1
Switch(config-pmap)# class cm-interface-1
Switch(config-pmap-c)# police 9000000 9000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# policy-map vlan-plcm1
Switch(config-pmap)# class cm-1
Switch(config-pmap-c)# set dscp 7
Switch(config-pmap-c)# service-policy port-plcm1
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface vlan 10
Switch(config-if)# service-policy input vlan-plcm1
```
Classifying, Policing, and Marking Ingress Traffic by Using Aggregate Policers

By using an aggregate policer, you can create a policer that is shared by multiple traffic classes within the same policy map. However, you cannot use the aggregate policer across different policy maps or ports.

You can configure aggregate policers only in nonhierarchical single-level policy maps.

Before beginning this procedure, make sure that you have created the class map to isolate traffic. For more information, see the “Classifying Ingress Traffic by Using ACLs” section on page 34-63 and the “Classifying Ingress Traffic by Using Class Maps” section on page 34-67.

Beginning in privileged EXEC mode, follow these steps to create an aggregate policer for inbound traffic:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>mls qos aggregate-policer aggregate-policer-name rate-bps burst-byte exceed-action { drop</td>
<td>policed-dscp-transmit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- For aggregate-policer-name, specify the name of the aggregate policer. - For rate-bps, specify average traffic rate in bps. The range is 8000 to 1000000000. - For burst-byte, specify the normal burst size in bytes. The range is 8000 to 1000000. - Specify the action to take when the rates are exceeded. Use the exceed-action drop keywords to drop the packet. Use the exceed-action policed-dscp-transmit keywords to mark down the DSCP value (through the policed-DSCP map) and send the packet. For more information, see the “Configuring the Policed-DSCP Map” section on page 34-83.</td>
</tr>
<tr>
<td>3</td>
<td>policy-map policy-map-name</td>
<td>Create a policy map by entering the policy-map name, and enter policy-map configuration mode. For more information, see the “Classifying, Policing, and Marking Ingress Traffic by Using Nonhierarchical Single-Level Policy Maps” section on page 34-69.</td>
</tr>
<tr>
<td>4</td>
<td>class class-name</td>
<td>Specify the name of the class whose traffic policy you want to create or change, and enter policy-map class configuration mode. By default, no traffic classes are defined.</td>
</tr>
<tr>
<td>5</td>
<td>police aggregate aggregate-policer-name</td>
<td>Apply an aggregate policer to multiple classes in the same policy map. For aggregate-policer-name, enter the name specified in Step 2.</td>
</tr>
<tr>
<td>6</td>
<td>exit</td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td>7</td>
<td>interface interface-id</td>
<td>Specify the port to attach to the policy map, and enter interface configuration mode.</td>
</tr>
</tbody>
</table>
Configuring Standard QoS

To remove the specified aggregate policer from a policy map, use the **no police aggregate aggregate-policer-name** policy-map class configuration command. To delete an aggregate policer and its parameters, use the **no mls qos aggregate-policer aggregate-policer-name** global configuration command.

This example shows how to create an aggregate policer and attach it to multiple classes within a policy map. In the configuration, the IP ACLs permit traffic from network 10.1.0.0 and from host 11.3.1.1. For traffic coming from network 10.1.0.0, the DSCP in the inbound packets is trusted. For traffic coming from host 11.3.1.1, the DSCP in the packet is changed to 56. The traffic rate from the 10.1.0.0 network and from host 11.3.1.1 is policed. If the traffic exceeds an average rate of 48000 bps and a normal burst size of 8000 bytes, its DSCP is marked down (based on the policed-DSCP map) and sent. The ingress policy map is attached to a port.

```
Switch(config)# access-list 1 permit 10.1.0.0 0.0.255.255
Switch(config)# access-list 2 permit 11.3.1.1
Switch(config)# mls qos aggregate-police transmit1 48000 8000 exceed-action policed-dscp-transmit
Switch(config)# class-map ipclass1
Switch(config-cmap)# match access-group 1
Switch(config-cmap)# exit
Switch(config)# class-map ipclass2
Switch(config-cmap)# match access-group 2
Switch(config-cmap)# exit
Switch(config)# policy-map aggflow1
Switch(config-pmap)# class ipclass1
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police aggregate transmit1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class ipclass2
Switch(config-pmap-c)# set dscp 56
Switch(config-pmap-c)# police aggregate transmit1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# exit
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# service-policy input aggflow1
```

### Configuring DSCP Maps

These sections describe how to configure the DSCP maps:

- **Configuring the CoS-to-DSCP Map, page 34-81** (optional)
- **Configuring the IP-Precedence-to-DSCP Map, page 34-82** (optional)
- **Configuring the Policed-DSCP Map, page 34-83** (optional, unless the null settings in the map are not appropriate)
All the maps, except the DSCP-to-DSCP-mutation map, are globally defined and are applied to all ports.

**Configuring the CoS-to-DSCP Map**

You use the CoS-to-DSCP map to map CoS values in inbound packets to a DSCP value that QoS uses internally to represent the priority of the traffic.

Table 34-13 shows the CoS-to-DSCP map.

<table>
<thead>
<tr>
<th>CoS Value</th>
<th>DSCP Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>2</td>
<td>16</td>
</tr>
<tr>
<td>3</td>
<td>24</td>
</tr>
<tr>
<td>4</td>
<td>32</td>
</tr>
<tr>
<td>5</td>
<td>40</td>
</tr>
<tr>
<td>6</td>
<td>48</td>
</tr>
<tr>
<td>7</td>
<td>56</td>
</tr>
</tbody>
</table>

If these values are not appropriate for your network, you need to modify them.

Beginning in privileged EXEC mode, follow these steps to modify the CoS-to-DSCP map. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>mls qos map cos-dscp dscp1...dscp8</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>show mls qos maps cos-dscp</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To return to the default map, use the **no mls qos cos-dscp** global configuration command.
This example shows how to modify and display the CoS-to-DSCP map:

```
Switch(config)# mls qos map cos-dscp 10 15 20 25 30 35 40 45
Switch(config)# end
Switch# show mls qos maps cos-dscp

Cos-dscp map:
   cos:  0 1 2 3 4 5 6 7
   --------------------------------
   dscp: 10 15 20 25 30 35 40 45
```

### Configuring the IP-Precedence-to-DSCP Map

You use the IP-precedence-to-DSCP map to map IP precedence values in inbound packets to a DSCP value that QoS uses internally to represent the priority of the traffic.

Table 34-14 shows the IP-precedence-to-DSCP map:

<table>
<thead>
<tr>
<th>IP Precedence Value</th>
<th>DSCP Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>2</td>
<td>16</td>
</tr>
<tr>
<td>3</td>
<td>24</td>
</tr>
<tr>
<td>4</td>
<td>32</td>
</tr>
<tr>
<td>5</td>
<td>40</td>
</tr>
<tr>
<td>6</td>
<td>48</td>
</tr>
<tr>
<td>7</td>
<td>56</td>
</tr>
</tbody>
</table>

If these values are not appropriate for your network, you need to modify them.

Beginning in privileged EXEC mode, follow these steps to modify the IP-precedence-to-DSCP map. This procedure is optional.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>mls qos map ip-prec-dscp</td>
<td>Modify the IP-precedence-to-DSCP map.</td>
</tr>
<tr>
<td></td>
<td>dscp1...dscp8</td>
<td>For <code>dscp1...dscp8</code>, enter eight DSCP values that correspond to the IP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>precedence values 0 to 7. Separate each DSCP value with a space.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The DSCP range is 0 to 63.</td>
</tr>
<tr>
<td>3</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>4</td>
<td>show mls qos maps ip-prec-dscp</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>5</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default map, use the `no mls qos ip-prec-dscp` global configuration command.
This example shows how to modify and display the IP-precedence-to-DSCP map:

Switch(config)# mls qos map ip-prec-dscp 10 15 20 25 30 35 40 45
Switch(config)# end
Switch# show mls qos maps ip-prec-dscp

IPPrecedence-dscp map:
  ipprec:   0  1  2  3  4  5  6  7
  -----------------------------
  dscp:   10 15 20 25 30 35 40 45

Configuring the Policed-DSCP Map

You use the policed-DSCP map to mark down a DSCP value to a new value as the result of an ingress policing and marking action.

The policed-DSCP map is a null map, which maps an inbound DSCP value to the same DSCP value.

Beginning in privileged EXEC mode, follow these steps to modify the policed-DSCP map. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>mls qos map policed-dscp dscp-list to mark-down-dscp</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
</tr>
<tr>
<td>Step 4</td>
<td>show mls qos maps policed-dscp</td>
</tr>
<tr>
<td>Step 5</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To return to the default map, use the no mls qos policed-dscp global configuration command.

This example shows how to map DSCP 50 to 57 to a marked-down DSCP value of 0:

Switch(config)# mls qos map policed-dscp 50 51 52 53 54 55 56 57 to 0
Switch(config)# end
Switch# show mls qos maps policed-dscp

Policed-dscp map:
  d1 :  d2 0  1  2  3  4  5  6  7  8  9
  -----------------------------------
  0 :    00 01 02 03 04 05 06 07 08 09
  1 :    10 11 12 13 14 15 16 17 18 19
  2 :    20 21 22 23 24 25 26 27 28 29
  3 :    30 31 32 33 34 35 36 37 38 39
  4 :    40 41 42 43 44 45 46 47 48 49
  5 :    00 00 00 00 00 00 00 00 00 58
  6 :    60 61 62 63
In this policed-DSCP map, the marked-down DSCP values are shown in the body of the matrix. The d1 column specifies the most-significant digit of the original DSCP; the d2 row specifies the least-significant digit of the original DSCP. The intersection of the d1 and d2 values provides the marked-down value. For example, an original DSCP value of 53 corresponds to a marked-down DSCP value of 0.

Configuring the DSCP-to-CoS Map

You use the DSCP-to-CoS map to generate a CoS value, which is used to select one of the four queues in the egress queue-set.

Table 34-15 shows the DSCP-to-CoS map.

<table>
<thead>
<tr>
<th>DSCP Value</th>
<th>CoS Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0–7</td>
<td>0</td>
</tr>
<tr>
<td>8–15</td>
<td>1</td>
</tr>
<tr>
<td>16–23</td>
<td>2</td>
</tr>
<tr>
<td>24–31</td>
<td>3</td>
</tr>
<tr>
<td>32–39</td>
<td>4</td>
</tr>
<tr>
<td>40–47</td>
<td>5</td>
</tr>
<tr>
<td>48–55</td>
<td>6</td>
</tr>
<tr>
<td>56–63</td>
<td>7</td>
</tr>
</tbody>
</table>

If these values are not appropriate for your network, you need to modify them.

Beginning in privileged EXEC mode, follow these steps to modify the DSCP-to-CoS map. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1  | configure terminal
|         | Enter global configuration mode. |
| Step 2  | mls qos map dscp-cos dscp-list to cos
|         | Modify the DSCP-to-CoS map. |
|         | • For dscp-list, enter up to eight DSCP values separated by spaces. |
|         | • For cos, enter the CoS value to which the DSCP values correspond. |
|         | The DSCP range is 0 to 63; the CoS range is 0 to 7. |
| Step 3  | end
|         | Return to privileged EXEC mode. |
| Step 4  | show mls qos maps dscp-to-cos
|         | Verify your entries. |
| Step 5  | copy running-config startup-config
|         | (Optional) Save your entries in the configuration file. |

To return to the default map, use the no mls qos dscp-cos global configuration command.
This example shows how to map DSCP values 0, 8, 16, 24, 32, 40, 48, and 50 to CoS value 0 and to display the map:

Switch(config)# mls qos map dscp-cos 0 8 16 24 32 40 48 50 to 0
Switch(config)# end
Switch# show mls qos maps dscp-cos
Dscp-cos map:
  d1 :  d2 0 1 2 3 4 5 6 7 8 9
  -------------------------------
  0 :    00 00 00 00 00 00 00 00 00 01
  1 :    01 01 01 01 01 01 00 02 02 02
  2 :    02 02 02 02 02 02 03 03 03 03
  3 :    03 03 03 03 03 03 04 04 04 04
  4 :    00 05 05 05 05 05 06 06 06 06
  5 :    00 06 06 06 06 06 07 07 07 07
  6 :    07 07 07 07

Note In the above DSCP-to-CoS map, the CoS values are shown in the body of the matrix. The d1 column specifies the most-significant digit of the DSCP; the d2 row specifies the least-significant digit of the DSCP. The intersection of the d1 and d2 values provides the CoS value. For example, in the DSCP-to-CoS map, a DSCP value of 08 corresponds to a CoS value of 0.

### Configuring the DSCP-to-DSCP-Mutation Map

If two QoS domains have different DSCP definitions, use the DSCP-to-DSCP-mutation map to translate one set of DSCP values to match the definition of another domain. You apply the DSCP-to-DSCP-mutation map to the receiving port (ingress mutation) at the boundary of a QoS administrative domain.

With ingress mutation, the new DSCP value overwrites the one in the packet, and QoS treats the packet with this new value. The switch sends the packet out with the new DSCP value.

You can configure multiple DSCP-to-DSCP-mutation maps and apply them to traffic received on a port. The DSCP-to-DSCP-mutation map is a null map, which maps an inbound DSCP value to the same DSCP value.

Beginning in privileged EXEC mode, follow these steps to modify the DSCP-to-DSCP-mutation map. This procedure is optional.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>mls qos map dscp-mutation dscp-mutation-name in-dscp to out-dscp</td>
<td>Modify the DSCP-to-DSCP-mutation map.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- For dscp-mutation-name, enter the mutation map name. You can create more than one map by specifying a new name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- For in-dscp, enter up to eight DSCP values separated by spaces. Then enter the to keyword.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- For out-dscp, enter a single DSCP value.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The DSCP range is 0 to 63.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>interface interface-id</td>
<td>Specify the port to which to attach the map, and enter interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Valid interfaces include physical ports.</td>
</tr>
</tbody>
</table>
Chapter 34      Configuring QoS

Configuring Standard QoS

To return to the default map, use the no mls qos dscp-mutation dscp-mutation-name global configuration command.

This example shows how to define the DSCP-to-DSCP-mutation map. All the entries that are not explicitly configured are not modified (remains as specified in the null map).

```
Switch(config)# mls qos map dscp-mutation mutation1 1 2 3 4 5 6 7 to 0
Switch(config)# mls qos map dscp-mutation mutation1 8 9 10 11 12 13 to 10
Switch(config)# mls qos map dscp-mutation mutation1 20 21 22 to 20
Switch(config)# mls qos map dscp-mutation mutation1 30 31 32 33 34 to 30
```

Switch(config-if)# mls qos trust dscp
Switch(config-if)# mls qos dscp-mutation mutation1

Switch(config-if)# end

Switch# show mls qos maps dscp-mutation mutation1

Dscp-dscp mutation map:
mutation1:
   d1 : d2 0 1 2 3 4 5 6 7 8 9
   0 : 00 00 00 00 00 00 00 10 10
   1 : 10 10 10 10 14 15 16 17 18 19
   2 : 20 20 20 23 24 25 26 27 28 29
   3 : 30 30 30 30 30 30 30 30 30 30
   4 : 40 41 42 43 44 45 46 47 48 49
   5 : 50 51 52 53 54 55 56 57 58 59
   6 : 60 61 62 63

Note
In the above DSCP-to-DSCP-mutation map, the mutated values are shown in the body of the matrix. The d1 column specifies the most-significant digit of the original DSCP; the d2 row specifies the least-significant digit of the original DSCP. The intersection of the d1 and d2 values provides the mutated value. For example, a DSCP value of 12 corresponds to a mutated value of 10.

Configuring Ingress Queue Characteristics

Single-level input policy maps are supported only on SVIs and standard physical ports. Depending on the complexity of your network and your QoS solution, you might need to perform all of the tasks in the next sections. You will need to make decisions about these characteristics:

- Which packets are assigned (by DSCP or CoS value) to each queue?
- What drop percentage thresholds apply to each queue, and which CoS or DSCP values map to each threshold?
- How much of the available buffer space is allocated between the queues?

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4 mls qos trust dscp</td>
<td>Configure the ingress port as a DSCP-trusted port. By default, the port is not trusted.</td>
</tr>
<tr>
<td>Step 5 mls qos dscp-mutation</td>
<td>Apply the map to the specified ingress DSCP-trusted port. For dscp-mutation-name, enter the mutation map name specified in Step 2.</td>
</tr>
<tr>
<td>Step 6 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 7 show mls qos maps dscp-mutation</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 8 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
- How much of the available bandwidth is allocated between the queues?
- Is there traffic (such as voice) that should be given high priority?

These sections describe how to configure ingress queue characteristics:
- Mapping DSCP or CoS Values to an Ingress Queue and Setting WTD Thresholds, page 34-87 (optional)
- Allocating Buffer Space Between the Ingress Queues, page 34-88 (optional)
- Allocating Bandwidth Between the Ingress Queues, page 34-89 (optional)
- Configuring the Ingress Priority Queue, page 34-90 (optional)

**Mapping DSCP or CoS Values to an Ingress Queue and Setting WTD Thresholds**

You can prioritize inbound traffic by placing packets with particular DSCP or CoS values into certain queues and by adjusting the queue thresholds so that packets with lower priorities are dropped.

Beginning in privileged EXEC mode, follow these steps to map DSCP or CoS values to an ingress queue and to set WTD thresholds. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Map DSCP or CoS values to an ingress queue and to a threshold ID.</td>
</tr>
<tr>
<td>mls qos srr-queue input dscp-map queue queue-id threshold threshold-id dscp1...dscp8</td>
<td>By default, DSCP values 0–39 and 48–63 are mapped to queue 1 and threshold 1. DSCP values 40–47 are mapped to queue 2 and threshold 1.</td>
</tr>
<tr>
<td>or mls qos srr-queue input cos-map queue queue-id threshold threshold-id cos1...cos8</td>
<td>By default, CoS values 0–4, 6, and 7 are mapped to queue 1 and threshold 1. CoS value 5 is mapped to queue 2 and threshold 1.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Assign the two WTD threshold percentages for (threshold 1 and 2) to an ingress queue. The default, both thresholds are set to 100 percent.</td>
</tr>
<tr>
<td>mls qos srr-queue input threshold queue-id threshold-percentage1 threshold-percentage2</td>
<td>- For queue-id, the range is 1 to 2.</td>
</tr>
<tr>
<td></td>
<td>- For threshold-percentage1, the range is 1 to 3. The drop-threshold percentage for threshold 3 is predefined. It is set to the queue-full state.</td>
</tr>
<tr>
<td></td>
<td>- For dscp1...dscp8, enter up to eight values, and separate each value with a space. The range is 0 to 63.</td>
</tr>
<tr>
<td></td>
<td>- For cos1...cos8, enter up to eight values, and separate each value with a space. The range is 0 to 7.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td>Assign the two WTD threshold percentages for (threshold 1 and 2) to an ingress queue. The default, both thresholds are set to 100 percent.</td>
</tr>
<tr>
<td>mls qos srr-queue input threshold queue-id threshold-percentage1 threshold-percentage2</td>
<td>- For queue-id, the range is 1 to 2.</td>
</tr>
<tr>
<td></td>
<td>- For threshold-percentage1 threshold-percentage2, the range is 1 to 100. Separate each value with a space.</td>
</tr>
<tr>
<td></td>
<td>Each threshold value is a percentage of the total number of queue descriptors allocated for the queue.</td>
</tr>
</tbody>
</table>

Return to privileged EXEC mode.
Chapter 34  Configuring QoS

Configuring Standard QoS

To return to the default CoS input queue threshold map or the DSCP input queue threshold map, use the `no mls qos srr-queue input cos-map` or the `no mls qos srr-queue input dscp-map` global configuration command. To return to the default WTD threshold percentages, use the `no mls qos srr-queue input threshold queue-id` global configuration command.

This example shows how to map DSCP values 0 to 6 to ingress queue 1 and to threshold 1 with a drop threshold of 50 percent. It maps DSCP values 20 to 26 to ingress queue 1 and to threshold 2 with a drop threshold of 70 percent.

```
Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 1 0 1 2 3 4 5 6
Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 2 20 21 22 23 24 25 26
Switch(config)# mls qos srr-queue input threshold 1 50 70
```

In this example, the DSCP values (0 to 6) are assigned the WTD threshold of 50 percent and will be dropped sooner than the DSCP values (20 to 26) assigned to the WTD threshold of 70 percent.

Allocating Buffer Space Between the Ingress Queues

You define the ratio (allocate the amount of space) with which to divide the ingress buffers between the two queues. The buffer and the bandwidth allocation control how much data can be buffered before packets are dropped.

Beginning in privileged EXEC mode, follow these steps to allocate the buffers between the ingress queues. This procedure is optional.

```
Step 1 configure terminal
Enter global configuration mode.

Step 2 mls qos srr-queue input buffers percentage1 percentage2
Allocate the buffers between the ingress queues
By default, 90 percent of the buffers are allocated to queue 1, and 10 percent of the buffers are allocated to queue 2.
For `percentage1 percentage2`, the range is 0 to 100. Separate each value with a space.
You should allocate the buffers so that the queues can handle any inbound bursty traffic.

Step 3 end
Return to privileged EXEC mode.
```
Configuring Standard QoS

To return to the default setting, use the `no mls qos srr-queue input buffers` global configuration command.

This example shows how to allocate 60 percent of the buffer space to ingress queue 1 and 40 percent of the buffer space to ingress queue 2:

```plaintext
Switch(config)# mls qos srr-queue input buffers 60 40
```

Allocating Bandwidth Between the Ingress Queues

You need to specify how much of the available bandwidth is allocated between the ingress queues. The ratio of the weights is the ratio of the frequency in which the SRR scheduler sends packets from each queue to the internal ring. The bandwidth and the buffer allocation control how much data can be buffered before packets are dropped. On ingress queues, SRR operates only in shared mode.

Beginning in privileged EXEC mode, follow these steps to allocate bandwidth between the ingress queues. This procedure is optional.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>mls qos srr-queue input bandwidth weight1 weight2</td>
<td>Assign shared round robin weights to the ingress queues. The default setting for <code>weight1</code> and <code>weight2</code> is 4 (1/2 of the bandwidth is equally shared between the two queues). For <code>weight1</code> and <code>weight2</code>, the range is 1 to 100. Separate each value with a space. SRR services the priority queue for its configured weight as specified by the <code>bandwidth</code> keyword in the <code>mls qos srr-queue input priority-queue queue-id bandwidth weight</code> global configuration command. Then, SRR shares the remaining bandwidth with both ingress queues and services them as specified by the weights configured with the <code>mls qos srr-queue input bandwidth weight1 weight2</code> global configuration command. For more information, see the “Configuring the Ingress Priority Queue” section on page 34-90.</td>
</tr>
<tr>
<td>3</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>4</td>
<td>show mls qos interface queueing</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>5</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default setting, use the `no mls qos srr-queue input bandwidth` global configuration command.
This example shows how to assign the ingress bandwidth to the queues. Priority queuing is disabled, and the shared bandwidth ratio allocated to queue 1 is 25/(25+75) and to queue 2 is 75/(25+75).

```
Switch(config)# mls qos srr-queue input priority-queue 2 bandwidth 0
Switch(config)# mls qos srr-queue input bandwidth 25 75
```

### Configuring the Ingress Priority Queue

You should use the ingress priority queue only for traffic that needs to be expedited (for example, voice traffic, which needs minimum delay and jitter).

The priority queue is guaranteed part of the bandwidth to reduce the delay and jitter under heavy network traffic on an oversubscribed ring (when there is more traffic than the backplane can carry, and the queues are full and dropping frames).

SRR services the priority queue for its configured weight as specified by the `bandwidth` keyword in the `mls qos srr-queue input priority-queue queue-id bandwidth weight` global configuration command. Then, SRR shares the remaining bandwidth with both ingress queues and services them as specified by the weights configured with the `mls qos srr-queue input bandwidth weight1 weight2` global configuration command.

Beginning in privileged EXEC mode, follow these steps to configure the ingress priority queue. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
</tbody>
</table>
| **Step 2** | mls qos srr-queue input priority-queue queue-id bandwidth weight | Assign a queue as the priority queue and guarantee bandwidth on the internal ring if the ring is congested.
- By default, the priority queue is queue 2, and 10 percent of the bandwidth is allocated to it.
- For `queue-id`, the range is 1 to 2.
- For `bandwidth weight`, assign the bandwidth percentage of the internal ring. The range is 0 to 40. The amount of bandwidth that can be guaranteed is restricted because a large value affects the entire ring and can degrade performance. |
| **Step 3** | end | Return to privileged EXEC mode. |
| **Step 4** | show mls qos interface queueing | Verify your entries. |
| or | show mls qos input-queue |
| **Step 5** | copy running-config startup-config | (Optional) Save your entries in the configuration file. |

To return to the default setting, use the `no mls qos srr-queue input priority-queue queue-id` global configuration command. To disable priority queuing, set the bandwidth weight to 0, for example, `mls qos srr-queue input priority-queue queue-id bandwidth 0`. 
This example shows how to assign the ingress bandwidths to the queues. Queue 1 is the priority queue with 10 percent of the bandwidth allocated to it. The bandwidth ratios allocated to queues 1 and 2 is 4/(4+4). SRR services queue 1 (the priority queue) first for its configured 10 percent bandwidth. Then SRR equally shares the remaining 90 percent of the bandwidth between queues 1 and 2 by allocating 45 percent to each queue.

Switch(config)# mls qos srr-queue input priority-queue 1 bandwidth 10
Switch(config)# mls qos srr-queue input bandwidth 4 4

Configuring Egress Queue-Set Characteristics

Single-level output policy maps are supported only on SVIs and ES ports. Depending on the complexity of your network and your QoS solution, you might need to perform all of the tasks in the next sections. You will need to make decisions about these characteristics:

- Which packets are mapped by DSCP or CoS value to each queue and threshold ID?
- What drop percentage thresholds apply to the queue-set (four egress queues per port), and how much reserved and maximum memory is needed for the traffic type?
- How much of the fixed buffer space is allocated to the queue-set?
- Does the bandwidth of the port need to be rate limited?
- Is there traffic (such as voice) that should be given high priority?
- How often should the egress queue-set be serviced and which technique (shaped, shared, or both) should be used?

These sections describe how to configure egress queue-set characteristics:

- Allocating Buffer Space to and Setting WTD Thresholds for an Egress Queue-Set, page 34-91 (optional)
- Mapping DSCP or CoS Values to an Egress Queue-Set and to a Threshold ID, page 34-93 (optional)
- Configuring SRR Shaped Weights on an Egress Queue-Set, page 34-95 (optional)
- Configuring SRR Shared Weights on an Egress Queue-Set, page 34-96 (optional)
- Configuring the Egress Priority Queue, page 34-97 (optional)
- Limiting the Egress Bandwidth on a Queue-Set, page 34-97 (optional)

Allocating Buffer Space to and Setting WTD Thresholds for an Egress Queue-Set

You can guarantee the availability of buffers, set WTD thresholds, and configure the maximum memory allocation for a queue-set by using the `mls qos queue-set output qset-id threshold queue-id drop-threshold1 drop-threshold2 reserved-threshold maximum-threshold` global configuration command. Each threshold value is a percentage of the queue’s allocated buffers, which you specify by using the `mls qos queue-set output qset-id buffers allocation1 ... allocation4` global configuration command. The queues use WTD to support distinct drop percentages for different traffic classes.

Note

The egress queue-set settings are suitable for most situations. You should change them only when you have a thorough understanding of the queues and only if these settings do not meet your QoS solution.
Beginning in privileged EXEC mode, follow these steps to configure the memory allocation and drop thresholds for a queue-set. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>mls qos queue-set output qset-id buffers allocation1 ... allocation4</code></td>
<td>Allocate buffers to a queue-set. By, all allocation values are equally mapped among the four queues (25, 25, 25, 25). Each queue has 1/4 of the buffer space.</td>
</tr>
<tr>
<td></td>
<td>• For <code>qset-id</code>, enter the ID of the queue-set. The range is 1 to 2. Each port belongs to a queue-set, which defines all the characteristics of the four egress queues per port.</td>
</tr>
<tr>
<td></td>
<td>• For <code>allocation1</code>, <code>allocation3</code>, and <code>allocation4</code>, the range is 0 to 99. For <code>allocation2</code>, the range is 1 to 100 (including the CPU buffer).</td>
</tr>
<tr>
<td></td>
<td>Allocate buffers according to the importance of the traffic. For example, give a larger percentage of the buffer to the queue with the highest-priority traffic.</td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>mls qos queue-set output qset-id threshold queue-id drop-threshold1 drop-threshold2 reserved-threshold maximum-threshold</code></td>
<td>Configure the WTD thresholds, guarantee the availability of buffers, and configure the maximum memory allocation for the queue-set (four egress queues per port). By default, the WTD thresholds for queues 1, 3, and 4 are set to 100 percent. The thresholds for queue 2 are set to 200 percent. The reserved thresholds for queues 1, 2, 3, and 4 are set to 50 percent. The maximum thresholds for all queues are set to 400 percent.</td>
</tr>
<tr>
<td></td>
<td>• For <code>qset-id</code>, enter the ID of the queue-set specified in Step 2. The range is 1 to 2.</td>
</tr>
<tr>
<td></td>
<td>• For <code>queue-id</code>, enter the specific queue in the queue-set on which the command is performed. The range is 1 to 4.</td>
</tr>
<tr>
<td></td>
<td>• For <code>drop-threshold1</code> <code>drop-threshold2</code>, specify the two WTD thresholds expressed as a percentage of the allocated queue memory. The range is 1 to 400 percent.</td>
</tr>
<tr>
<td></td>
<td>• For <code>reserved-threshold</code>, enter the amount of memory to be guaranteed (reserved) for the queue expressed as a percentage of the allocated memory. The range is 1 to 100 percent.</td>
</tr>
<tr>
<td></td>
<td>• For <code>maximum-threshold</code>, enable a full queue to obtain more buffers than are reserved for it. This is the maximum memory the queue can have before the packets are dropped if the common pool is not empty. The range is 1 to 400 percent.</td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>interface interface-id</code></td>
<td>Specify the port, and enter interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 5</strong> <code>queue-set qset-id</code></td>
<td>Map the port to a queue-set. For <code>qset-id</code>, enter the ID of the queue-set specified in Step 2. The range is 1 to 2. The default is 1.</td>
</tr>
<tr>
<td><strong>Step 6</strong> end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
To return to the default setting, use the `no mls qos queue-set output qset-id buffers` global configuration command. To return to the default WTD threshold percentages, use the `no mls qos queue-set output qset-id threshold [queue-id]` global configuration command.

This example shows how to map a port to queue-set 2. It allocates 40 percent of the buffer space to egress queue 1 and 20 percent each to egress queues 2, 3, and 4. It configures the drop thresholds for queue 2 to 40 and 60 percent of the allocated memory, guarantees (reserves) 100 percent of the allocated memory, and configures 200 percent as the maximum memory that this queue can have before packets are dropped.

```
Switch(config)# mls qos queue-set output 2 buffers 40 20 20 20
Switch(config)# mls qos queue-set output 2 threshold 2 40 60 100 200
Switch(config)# interface fastethernet1/0/1
Switch(config-if)# queue-set 2
```

### Mapping DSCP or CoS Values to an Egress Queue-Set and to a Threshold ID

You can prioritize traffic by placing packets with particular DSCP or CoS values into certain queues and by adjusting the queue thresholds so that packets with lower priorities are dropped.

- **Note**

  The egress queue-set settings are suitable for most situations. You should change them only when you have a thorough understanding of the queues and only if these settings do not meet your QoS solution.
Beginning in privileged EXEC mode, follow these steps to map DSCP or CoS values to an egress queue and to a threshold ID. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>mls qos srr-queue output dscp-map queue queue-id threshold threshold-id dscp1...dscp8</td>
</tr>
<tr>
<td></td>
<td>or mls qos srr-queue output cos-map queue queue-id threshold threshold-id cos1...cos8</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>show mls qos maps</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>copy running-config startup-config</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Configuring SRR Shaped Weights on an Egress Queue-Set

You can specify how much of the available bandwidth is allocated to each queue in the queue-set. The ratio of the weights is the ratio of frequency in which the SRR scheduler sends packets from a standard port.

Note

SRR shaping is not supported on the ES ports; however, you can configure average-rate shaping. For more information, see the “Configuring Shaping” section on page 34-129.

You can configure the egress queues for shaped weights, shared weights, or both. Use shaping to smooth bursty traffic or to provide a smoother output over time. For conceptual information, see the “SRR Shaping and Sharing” section on page 34-19. For configuration information, see the “Configuring SRR Shared Weights on an Egress Queue-Set” section on page 34-96.

Note

The egress queue-set settings are suitable for most situations. You should change them only when you have a thorough understanding of the queues and only if these settings do not meet your QoS solution.

Beginning in privileged EXEC mode, follow these steps to assign the shaped weights and to enable bandwidth shaping on a standard port mapped to the four egress queues. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>srr-queue bandwidth shape weight1 weight2 weight3 weight4</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
</tr>
<tr>
<td>Step 5</td>
<td>show mls qos interface interface-id queueing</td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To return to the default setting, use the no srr-queue bandwidth shape interface configuration command.
This example shows how to configure bandwidth shaping on queue 1. Because the weight ratios for queues 2, 3, and 4 are set to 0, these queues operate in shared mode. The bandwidth weight for queue 1 is 1/8, which is 12.5 percent.

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# srr-queue bandwidth shape 8 0 0 0
```

### Configuring SRR Shared Weights on an Egress Queue-Set

In shared mode, the queues in the queue-set share the bandwidth among them according to the configured weights. The bandwidth is guaranteed at this level but not limited to it. For example, if a queue empties and does not require a share of the link, the remaining queues can expand into the unused bandwidth and share it among them. With sharing, the ratio of the weights controls the frequency of dequeuing; the absolute values are meaningless.

**Note**
The egress queue-set settings are suitable for most situations. You should change them only when you have a thorough understanding of the queues and only if these settings do not meet your QoS solution.

Beginning in privileged EXEC mode, follow these steps to assign the shared weights and to enable bandwidth sharing on a port mapped to the four egress queues. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Enter global configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Specify a port, and enter interface configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>srr-queue bandwidth share weight1 weight2 weight3 weight4</td>
</tr>
<tr>
<td>Assign SRR weights to the egress queues.</td>
<td></td>
</tr>
<tr>
<td>By default, all four weights are 25 (1/4 of the bandwidth is allocated to each queue).</td>
<td></td>
</tr>
<tr>
<td>For weight1 weight2 weight3 weight4, enter the weights to control the ratio of the frequency in which the SRR scheduler sends packets. Separate each value with a space. The range is 1 to 255.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>end</td>
</tr>
<tr>
<td>Return to privileged EXEC mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>show mls qos interface interface-id queueing</td>
</tr>
<tr>
<td>Verify your entries.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>copy running-config startup-config</td>
</tr>
<tr>
<td>(Optional) Save your entries in the configuration file.</td>
<td></td>
</tr>
</tbody>
</table>

To return to the default setting, use the **no srr-queue bandwidth share** interface configuration command.

This example shows how to configure the weight ratio of the SRR scheduler running on an egress port. Four queues are used, and the bandwidth ratio allocated for each queue in shared mode is 1/(1+2+3+4), 2/(1+2+3+4), 3/(1+2+3+4), and 4/(1+2+3+4), which is 10 percent, 20 percent, 30 percent, and 40 percent for queues 1, 2, 3, and 4. This means that queue 4 has four times the bandwidth of queue 1, twice the bandwidth of queue 2, and one-and-a-third times the bandwidth of queue 3.

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# srr-queue bandwidth share 1 2 3 4
```
Configuring the Egress Priority Queue

Beginning in Cisco IOS Release 12.1(14)AX2, you can ensure that certain packets have priority over all others by queuing them in the egress priority queue on a port. SRR services this queue until it is empty and before servicing the other queues.

If you expect that the traffic classes mapped to the egress priority queue will pass through an ES port, you also might want to map those classes for strict-priority queuing as described in the “Enabling LLQ” section on page 34-127.

Beginning in privileged EXEC mode, follow these steps to enable the egress priority queue. This procedure is optional.

<table>
<thead>
<tr>
<th>Command3</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1  configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2  interface interface-id</td>
<td>Specify a port, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3  priority-queue out</td>
<td>Enable the egress priority queue, which is disabled by default.</td>
</tr>
<tr>
<td></td>
<td>When you configure this command, the SRR weight and queue size ratios</td>
</tr>
<tr>
<td></td>
<td>are affected because there is one fewer queue participating in SRR. This</td>
</tr>
<tr>
<td></td>
<td>means that weight1 in the srr-queue bandwidth shape or the srr-queue</td>
</tr>
<tr>
<td></td>
<td>bandwidth share command is not used in the ratio calculation.</td>
</tr>
<tr>
<td>Step 4  end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5  show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 6  copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable the egress priority queue, use the no priority-queue out interface configuration command.

This example shows how to enable the egress priority queue when the SRR weights are configured. The egress expedite queue overrides the configured SRR weights.

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# srr-queue bandwidth shape 25 0 0 0
Switch(config-if)# srr-queue bandwidth share 30 20 25 25
Switch(config-if)# priority-queue out
Switch(config-if)# end
```

Limiting the Egress Bandwidth on a Queue-Set

You can limit the egress bandwidth on a standard port mapped to a queue-set. For example, if a customer pays only for a small percentage of a high-speed link, you can limit the bandwidth to that amount.

Note

The egress queue-set settings are suitable for most situations. You should change them only when you have a thorough understanding of the queues and only if these settings do not meet your QoS solution.
Beginning in privileged EXEC mode, follow these steps to limit the egress bandwidth on a standard port. This procedure is optional.

**Configuring Marking and Queuing for CPU-Generated Traffic**

Beginning in privileged EXEC mode, follow these steps to configure marking and queuing of CPU-generated traffic. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>srr-queue bandwidth limit weight1</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
</tr>
<tr>
<td>Step 5</td>
<td>show mls qos interface [interface-id] queueing</td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To return to the default setting, use the **no srr-queue bandwidth limit** interface configuration command.

This example shows how to limit the bandwidth on a standard port to 80 percent:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# srr-queue bandwidth limit 80
```

When you configure this command to 80 percent, the port is idle 20 percent of the time. The line rate drops to 80 percent of the connected speed, which is 800 Mb/s. These values are not exact because the hardware adjusts the line rate in increments of six.

**Configuring Marking and Queuing for CPU-Generated Traffic**

Beginning in privileged EXEC mode, follow these steps to configure marking and queuing of CPU-generated traffic. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 3</td>
<td>cpu traffic qos cos {cos-value</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
</tbody>
</table>
To disable any command, use the no form of the command.

**Example 1**

This example shows how to mark the CoS of CPU-generated IP traffic (including IP-SLA and TWAMP) based on the packet DSCP value and to configure egress queuing based on the DSCP value.

The example has these results:

- All CPU-generated IP traffic queues on the egress port based on the IP-DSCP value.
- All IP traffic with the DSCP value ef (46), which simulates voice traffic, is assigned the CoS value 5.
- All IP traffic with the DSCP values af41 (34), af42 (36) and af43 (38) is assigned the CoS value 4.
- All Internet Control Protocol traffic with the DSCP values 48 and 56 are assigned the CoS value 7.
- The rest of the IP and non-IP traffic is processed according to the default configuration.
- Queue the DSCP value 46 to queue 1 threshold 1.
- Queue the DSCP values 34 36 38 to queue 2 threshold 3.
- Queue the DSCP values 48 56 to queue 4 threshold 2.
- All other CPU traffic egress through the default queue 2 and threshold 1.
Maps:

```
Switch(config)# mls qos
Switch(config)# mls qos map dscp-cos 46 to 5
Switch(config)# mls qos map dscp-cos 34 36 38 to 4
Switch(config)# mls qos map dscp-cos 48 56 to 7
```

CPU QoS:

```
Switch(config)# cpu traffic qos dscp trust
```

Queuing:

```
Switch(config)# mls qos srr-queue output dscp-map queue 1 threshold 1 46
Switch(config)# mls qos srr-queue output dscp-map queue 2 threshold 3 34 36 38
Switch(config)# mls qos srr-queue output dscp-map queue 4 threshold 2 48 56
```

Example 2
This example shows how to mark the DSCP of CPU-generated IP traffic (including IP-SLA and TWAMP) based on the DSCP value in the packet.

The example has these results:

- All IP traffic with the DSCP value 0 is assigned DSCP value 30.
- All IP traffic with the DSCP values af41 (34), af42 (36) and af43 (38) are assigned DSCP value 48.
- All other IP and non-IP traffic is processed by the default configuration.

Maps:

```
Switch(config)# mls qos
Switch(config)# mls qos map dscp-mutation mapname 0 to 30
Switch(config)# mls qos map dscp-mutation mapname 34 36 38 to 48
```

CPU QoS:

```
Switch(config)# cpu traffic qos dscp dscp-mutation mapname
```

Example 3
This example shows how to mark the precedence of CPU-generated IP traffic (including IP-SLA and TWAMP) based on the precedence value in the packet.

The example has these results:

- All CPU generated IP traffic with the precedence value 0 is assigned precedence value 3.
- All CPU generated IP traffic with the precedence values 2, 3 and 4 is assigned precedence value 6.
- All other IP and non-IP traffic is processed by the default configuration.

Maps:

```
Switch(config)# mls qos
Switch(config)# mls qos map dscp-mutation mapname 0 to 24
Switch(config)# mls qos map dscp-mutation mapname 16 24 32 to 48
```

CPU QoS:
Switch(config)# cpu traffic qos precedence precedence-mutation mapname

Note
IP-DSCP and IP-precedence are related. To mark the precedence value of an IP packet based on the incoming packet precedence value, an equivalent DSCP-mutation map needs to be configured and used with the cpu traffic qos precedence precedence-mutation command. Queuing is based on the IP-DSCP value of the packet.

Example 4
This example shows how to mark the DSCP of CPU-generated IP traffic (including IP-SLA and TWAMP) based on the CoS value in the packet and to configure egress queuing based on the CoS value. The example has these results:

- All CPU-generated IP traffic is queued on the egress port based on the CoS value.
- All IP traffic with the CoS value 0 is assigned DSCP value 30.
- All IP traffic with the CoS values 6 and 7 is assigned DSCP value 56.
- All other IP and non-IP traffic is processed by the default configuration.
- Queues the CoS value 0 to queue 1 threshold 1.
- Queues the CoS values 6 and 7 to queue 2 threshold 3.
- All other CPU traffic egresses through the default queue 2 and threshold 1.

Maps:
Switch(config)# mls qos
Switch(config)# mls qos map cos-dscp 0 to 30
Switch(config)# mls qos map cos-dscp 6 7 to 56

CPU QoS:
Switch(config)# cpu traffic qos cos trust

Queuing:
Switch(config)# mls qos srr-queue output cos-map queue 1 threshold 1 0
Switch(config)# mls qos srr-queue output cos-map queue 2 threshold 3 6 7

Example 5
This example shows how to mark the CoS of CPU-generated IP traffic (including IP-SLA and TWAMP) based on the precedence value in the packet and to configure egress queuing based on the DSCP value. The example has these results:

- All CPU-generated IP traffic is queued on the egress port based on the IP-DSCP value.
- All IP traffic with the precedence value 3, which simulates voice traffic, is assigned CoS value 5.
- All IP traffic with the precedence values 4 and 5 are assigned CoS value 7.
- All other IP and non-IP traffic is processed by the default configuration.
- Queues the DSCP value 24 (equivalent to precedence value 3) to queue 1 threshold 1.
- Queues the DSCP values 32 and 40 (equivalent to precedence values 4 and 5) to queue 2 threshold 3.
- All other CPU traffic egresses through the default queue 2 and threshold 1.
Maps:

Switch(config)# mls qos
Switch(config)# mls qos map dscp-cos 24 to 5
Switch(config)# mls qos map dscp-cos 32 40 to 7

CPU QoS:

Switch(config)# cpu traffic qos precedence trust

Queuing:

Switch(config)# mls qos srr-queue output dscp-map queue 1 threshold 1 24
Switch(config)# mls qos srr-queue output dscp-map queue 2 threshold 3 32 40

Displaying Standard QoS Information

To display standard QoS information, use one or more of the privileged EXEC commands in Table 34-16:

Table 34-16 Commands for Displaying Standard QoS Information

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show class-map [class-map-name]</td>
<td>Display QoS class maps, which define the match criteria to classify traffic.</td>
</tr>
<tr>
<td>show cpu traffic qos</td>
<td>Display QoS parameters for control plane traffic.</td>
</tr>
<tr>
<td>show mls qos</td>
<td>Display global QoS configuration information.</td>
</tr>
<tr>
<td>show mls qos aggregate-policer [aggregate-policer-name]</td>
<td>Display the aggregate policer configuration.</td>
</tr>
<tr>
<td>show mls qos input-queue</td>
<td>Display QoS settings for the ingress queues.</td>
</tr>
<tr>
<td>show mls qos interface [interface-id] [buffers</td>
<td>policers</td>
</tr>
<tr>
<td>show mls qos queue-set [qset-id]</td>
<td>Display the egress queue-set settings.</td>
</tr>
<tr>
<td>show mls qos vlan vlan-id</td>
<td>Display the policy maps attached to an SVI.</td>
</tr>
<tr>
<td>show policy-map [policy-map-name [class class-map-name]]</td>
<td>Display QoS policy maps, which define the traffic policy for a traffic class.</td>
</tr>
<tr>
<td>show policy-map interface interface-id [input]</td>
<td>Display the ingress policy-map name applied to the specified port.</td>
</tr>
</tbody>
</table>
Configuring Hierarchical QoS

You can configure hierarchical QoS (traffic classification, CBWFQ, LLQ, shaping, and two-rate, three-color policing) and apply it to inbound or outbound traffic on an ES port or on an EtherChannel made of ES ports.

Before configuring hierarchical QoS, you must have a thorough understanding of these items:

- The types of applications used and the traffic patterns on your network.
- Traffic characteristics and needs of your network. Is the traffic bursty? Do you need to reserve bandwidth for voice and video streams?
- Bandwidth requirements and speed of the network.
- Location of congestion points in the network.

These sections describe how to configure hierarchical QoS on your switch. Read these sections if traffic is flowing from a standard or an ES port to an Etherchannel ES port:

- Hierarchical QoS Configuration, page 34-103
- Hierarchical QoS Configuration Guidelines, page 34-103
- Hierarchical QoS Over EtherChannel Configuration Guidelines, page 34-105
- Configuring a Hierarchical QoS Policy, page 34-107 (required)

Hierarchical QoS Configuration

QoS is disabled.
No traffic classes, class maps, policy maps, or policers are defined.
LLQ is disabled.
CBWFQ is disabled.
Tail drop is enabled.
WRED is disabled.
Average-rate traffic shaping is disabled.

Hierarchical QoS Configuration Guidelines

These hierarchical QoS configuration guidelines apply to ingress and egress service-policies on an ES port or an ES EtherChannel (an EtherChannel consisting of ES ports)

**Note**
The switch does not support IPv6 features with ES-port specific features, such as hierarchical QoS.

- QoS must be enabled with the `mls qos` global configuration command for any hierarchical configuration to take effect. When enabled, QoS uses the default settings described in the “Standard QoS Configuration” section on page 34-50 and the “Hierarchical QoS Configuration” section on page 34-103. For detailed steps, see the “Enabling QoS Globally” section on page 34-56.
- Beginning with Cisco IOS Release 12.2(35)SE, you can attach a hierarchical service policy to an EtherChannel of ES ports. You can use the policy to configure hierarchical policies on ES ports without configuring QoS classification, policing, mapping, and queuing on the individual ES ports
in the EtherChannel. If you configure a hierarchical policy on an EtherChannel that has no ports and then add a standard port to the EtherChannel, the policy is removed from the EtherChannel. See the “Hierarchical QoS Over EtherChannel Configuration Guidelines” section on page 34-105 for more information about this feature.

- Class maps that contain ACLs are not supported in either an egress policy or in a hierarchical ingress policy attached to an ES port or EtherChannel. You cannot configure the match access-group acl-index-or-name class-map configuration command in a hierarchical policy map.

- To configure a class map that matches an IEEE 802.1Q tunneling pair (instead of matching a single VLAN), you must configure the class-map global configuration command with the match-all keyword. You must enter the match vlan command before the match vlan inner command.

- You cannot have the match vlan {vlan-id | inner vlan-id} and match {cos | inner} cos-list | ip dscp dscp-list | ip precedence ip-precedence-list | mpls experimental exp-list class-map configuration commands in the same class map.

- If you enter the match vlan or the match vlan inner command, the class-map match-any command is not supported.

- You cannot mix VLAN-level and class-level matches within a class map.

- When port trust policies are used with IEEE 802.1Q tunneling, all ports sharing the same tunnel VLAN must be configured with the same trust policy.

- Only one policy map per port is supported. You can attach one input hierarchical service policy and one output service policy per ES port or EtherChannel.

- You cannot apply an output policy map with only one level to an ingress ES port or EtherChannel.

- When a trust policy and a hierarchical ingress policy are both configured on an ES port or EtherChannel, the actions specified in the service policy are processed before the trust policy is applied.

- If an ingress hierarchical policy map includes the set policy-map class configuration command, the switch automatically applies the port trust state to the ES port or EtherChannel. The switch applies the port trust state to all inbound traffic on the port or EtherChannel, including traffic that does not match the traffic class. For example, if you enter the set cos new-cos command, the switch automatically configures the interface to trust CoS.

- If an input hierarchical policy map sets QoS values by using explicit set actions or policing actions, the ES port or EtherChannel must also have the appropriate trust policy configured. For example, if the policy modifies CoS, then the ES port or EtherChannel must trust CoS; if the policy modifies DSCP, the ES port must trust DSCP. If the ingress policy contains a mix of Layer 2 and Layer 3 QoS modifications, the policy cannot be attached.

- If an egress hierarchical policy map includes the set policy-map class configuration command, the port trust state is not affected. For example, setting the CoS to 2 only affects the CoS value of the packet, and the DSCP value of the packet is not modified based on the CoS-to-DSCP map.

- In an ingress policy map, you cannot combine Layer 2 and Layer 3 set actions because the port can trust only one value in the inbound packet. For example, the switch does not support this policy map:

  ```
policy-map pl
    class cos1
      police cir per 10 conform-action set-cos-transmit 3
      set dscp af22
  ```

- On an ES port or EtherChannel, the only limit to the number of policers configured in a hierarchical service-policy is the finite number of classes that can be configured. For more information, see the “Hierarchical Levels” section on page 34-30.
• If you configure the **conform-action**, **exceed-action**, **violate-action** in a two-rate ingress policer and set the CoS, DSCP, or IP precedence values of the packet by using the **set-cos-transmit new-cos**, **set-dscp-transmit new-dscp**, or the **set-prec-transmit new-prec** options, the switch automatically applies the port trust state to all traffic received on the ES port or EtherChannel, including traffic that does not match the traffic class with the two-rate policer.

• You cannot combine Layer 2 (**set-cos-transmit new-cos**) and Layer 3 (**set-dscp-transmit new-dscp**, or **set-prec-transmit new-prec**) actions in a two-rate ingress policer because the port can trust only one value in the inbound packet (CoS, DSCP, or IP precedence). For example, you cannot configure the **police cir percent 10 conform-action set-cos-transmit 3 exceed-action set-dscp-transmit af22** command. The **conform-action** sets the CoS value to 3, but the **exceed-action** sets the DSCP value to af22.

• Use the configuration procedures in this section to configure hierarchical multiple-level policies on ES ports or EtherChannels. Many of the configuration options are not supported in single-level policy maps attached to ES ports.

• If you want to use a hierarchical ingress single-level service-policy (for example, a two-rate ingress policer on an ES port or EtherChannel), you must create a second level in the hierarchy with only the class-default in the policy map. For example, in the policy map, specify **class-default** as the class name in the **class** policy-map configuration command.

• You can define a class policy to use either tail drop through the **queue-limit** policy-map class configuration command or to use WRED packet drop through the **random-detect** policy-map class configuration command. You cannot use the **queue-limit** and **random-detect** commands in the same class policy, but they can be used in two class policies in the same policy map.

• You cannot use **bandwidth**, **queue-limit**, **random-detect**, and **shape** policy-map class configuration commands with the **priority** policy-map class configuration command in the same class within the same policy map. However, you can use these commands in different classes in the same policy map. Within a policy map, you can give priority status to only one class.

• You must configure the **bandwidth** or the **shape** policy-map class configuration command before you configure either the **queue-limit** or the **random-detect** policy-map class configuration command in a class policy. You must configure the **bandwidth** or the **shape** command in the same policy map as the **queue-limit** or the **random-detect** command if the policy is not using the traffic class. If the policy is using the traffic class, you do not need to specify the **bandwidth** and **shape** commands in the policy map.

• A policy map can have all the class bandwidths specified in either kb/s or in percentages, but not a mix of both. You cannot specify bandwidth in kb/s in a child policy (configured through the **service-policy** policy-map class configuration command) and then specify bandwidth as a percentage in the parent policy.

• In a child policy map, the minimum bandwidth of each class map must be more than 0.01 percent of the total bandwidth of the parent policy map. When **class-default** class is not configured in the child policy map, this minimum bandwidth map is reserved for the **class-default** class.

• The total bandwidth configured in a child policy map cannot exceed the total bandwidth of the parent policy map.

### Hierarchical QoS Over EtherChannel Configuration Guidelines

Beginning with Cisco IOS Release 12.2(35)E, hierarchical QoS is supported on EtherChannels consisting of Catalyst 3750 Metro ES ports. When you configure an EtherChannel with both ES ports and apply a hierarchical policy to it, hierarchical QoS is applied to traffic flowing through both ports. After all hierarchical QoS rules (including policing, shaping, bandwidth, and priority) are applied,
packets are sent out of the correct physical interface. These rules apply to the entire EtherChannel pipe. In addition to hierarchical QoS, standard EtherChannel redundancy and load balancing takes place based on the type of configuration. Because EtherChannels are logical interfaces, there are some differences in hierarchical QoS over EtherChannels compared to hierarchical QoS over ES ports.

This section lists guidelines and features of hierarchical QoS over EtherChannel, including differences in behavior compared to ES ports. Cisco IOS Release 12.2(35)SE does not change hierarchical QoS on ES ports.

The switch does not support IPv6-related features with ES-port specific features, such hierarchical QoS.

- Hierarchical QoS is supported in both ingress and egress directions for EtherChannels.
- Hierarchical policies are supported only on EtherChannels made of ES ports; they are not supported on EtherChannels made of standard ports.
- You can attach a hierarchical policy to an EtherChannel made of ES ports only if no other policies are attached to the individual ES ports.
- You can attach a hierarchical policy to an EtherChannel that contains no ports. However, the policy is effective only when you add one or more ES ports to the EtherChannel.
- If an EtherChannel has only one active ES port, a hierarchical policy attached to the EtherChannel acts exactly like a hierarchical policy on the individual ES port.
- If you try to add a standard port to an empty EtherChannel that has a hierarchical policy attached to it, the port is added to the EtherChannel, but the hierarchical policy is removed. Hierarchical policies are supported only on EtherChannels with ES ports.
- Hierarchical QoS on an EtherChannel does not affect the EtherChannel load balancing. If both ES ports in an EtherChannel are active, traffic for the ports is queued for hierarchical QoS and then sent to the original target interface.
- Parameters for actions (such as bandwidth and policing) must all be configured as either absolute values or as percentages across all classes of the hierarchical policy map. The configuration determines whether the policy is a load-balancing or a redundancy application.
  - When you configure all hierarchical QoS parameters as absolute values, the total configurable bandwidth is limited to the bandwidth of one of the links (990,000,000 bits per second), which results in redundancy.
  - When you configure all hierarchical parameters as percentage values, you can configure 100 percent bandwidth. When both links are up, the bandwidth is approximately 2 Gigabits (two times 990,000,000 bits per second). If one link goes down, the bandwidth becomes 1 Gigabit and all policies are scaled down, although the percentages remain the same, which results in load balancing. The switch does not support percentage shaping for load balancing.
- For policing policies configured in percentages, an internal limitation sets the maximum policing parameter to 990,000,000 bits per second. If a link state change causes the policing value to be greater than this value, the policy is detached. Therefore, when you configure the percentage for an EtherChannel with both ES links, you should limit each policer to a maximum of 49 percent. However, you can configure multiple policers in the same policy or across parent and child policies with each configured to the 49 per cent maximum.
- These are the results of ES link state changes for hierarchical QoS parameters configured as absolute values or percentages:
– If you configure parameters in absolute values, the total guaranteed bandwidth cannot be greater than 990,000,000 bits per second. If one link in the EtherChannel goes down, all traffic goes in or out of the other physical interface instead of being distributed between the two ES ports. No values are recalculated, and there are no changes to hierarchical QoS parameters or policy enforcement.

– If you configure parameters in percentages and one link in the EtherChannel goes down, all absolute parameters are reduced by half, although the configured percentage remains the same. For bandwidth percentage configuration, all traffic is sent or received with the reduced bandwidth parameters distributed fairly. For policing percentage configuration, packets are dropped according to the reduced parameters so that other traffic is not affected.

• The switch does not support shaping percentages for hierarchical QoS for ES ports or EtherChannels. Therefore, you cannot configure policing or bandwidth in percentages with any type of shaping for policies applied to an EtherChannel.

• If you simultaneously attach both egress and ingress EtherChannel hierarchical policies, you must configure both policies in either absolute values or in percentages. You cannot configure an ingress policy with percentages and an egress policy with an absolute value, or the reverse.

Configuring a Hierarchical QoS Policy

These sections describe how to configure a hierarchical QoS policy to create a service policy that is attached to an ES port or to an EtherChannel made of ES ports.

Note

The switch does not support IPv6 features with ES-port specific features, such as hierarchical QoS.

For background information, see the “Hierarchical Levels” section on page 34-30, the “Hierarchical Classification Based on Traffic Classes and Traffic Policies” section on page 34-33, the “Hierarchical Policies and Marking” section on page 34-34, and the “Queueing and Scheduling of Hierarchical Queues” section on page 34-37. For configuration guidelines, see the “Hierarchical QoS Configuration Guidelines” section on page 34-103.

Depending on your network configuration and QoS solution, you must perform one or more of these tasks if you want classify, policy, mark, queue, or schedule traffic:

• Classifying Traffic by Using Hierarchical Class Maps, page 34-108 (required)
• Configuring a Hierarchical Two-Rate Traffic Policer, page 34-110 (optional)
• Configuring Class-Based Packet Marking in a Hierarchical Traffic Policy, page 34-114 (optional)
• Configuring CBWFQ and Tail Drop, page 34-116 (optional)
• Configuring CBWFQ and DSCP-Based WRED, page 34-119 (optional)
• Configuring CBWFQ and IP Precedence-Based WRED, page 34-123 (optional)
• Enabling LLQ, page 34-127 (optional)
• Configuring Shaping, page 34-129 (optional)
Classifying Traffic by Using Hierarchical Class Maps

You use the `class-map` global configuration command to create a class map for matching packets to the class whose name you specify. The class map isolates a specific traffic flow (class) from all other traffic by defining the criteria to use to match against a specific flow. The match criterion is defined with a match statement entered within the class-map configuration mode. Packets are compared to the match criteria configured for a class map. If a packet matches the specified criteria, the packet is considered a member of the class and is forwarded according to the QoS specifications set in the traffic policy.

Beginning in privileged EXEC mode, follow these steps to create a class-level class-map and to define the match criterion to classify traffic. This procedure is required. The examples that follow the procedure show how to create a class-level and a VLAN-level class-map.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>class-map [match-all</td>
</tr>
<tr>
<td></td>
<td>• (Optional) Use the <code>match-all</code> keyword to perform a logical-AND of all matching statements under this class map. All criteria in the class map must be matched.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) Use the <code>match-any</code> keyword to perform a logical-OR of all matching statements under this class map. One or more criteria must be matched.</td>
</tr>
<tr>
<td></td>
<td>• For <code>class-map-name</code>, specify the name of the class map.</td>
</tr>
<tr>
<td></td>
<td>If neither the <code>match-all</code> nor the <code>match-any</code> keyword is specified, the default is <code>match-all</code>. You must use the <code>match-all</code> keyword if you are matching an IEEE 802.1Q tunneling pair (instead of matching a single VLAN).</td>
</tr>
</tbody>
</table>
To delete an existing class map, use the `no class-map [match-all | match-any] class-map-name` global configuration command. To remove a match criterion, use the `no match [cos [inner] cos-list | ip dscp dscp-list | ip precedence ip-precedence-list | mpls experimental exp-list | vlan {vlan-id | inner vlan-id}]` class-map configuration command.

This example shows how to create a class-level class-map called `class3`, which matches traffic with IP-precedence values of 5, 6, and 7:

```
Switch(config)# class-map class3
Switch(config-cmap)# match ip precedence 5 6 7
```
Configuring Hierarchical QoS

This example shows how to create a VLAN-level class-map for IEEE 802.1Q tunneling called dot1q, which matches all traffic with an outer VLAN ID of 5 and an inner VLAN ID of 3 to 8:

```
Switch(config)# class-map match-all dot1q
Switch(config-cmap)# match vlan 5
Switch(config-cmap)# match vlan inner 3 - 8
```

This example shows how to create a VLAN-level class-map called vlan203, which matches traffic in VLAN 203:

```
Switch(config)# class-map match-all vlan203
Switch(config-cmap)# match vlan 203
```

Configuring a Hierarchical Two-Rate Traffic Policer

You can configure a two-rate traffic policer within a policy map at the class level, at the VLAN level, and at the physical level by using the `police cir` or the `police cir percent` policy-map class configuration command. At the physical level of the hierarchy, you can police only the class-level in a policy attached to an ES port or EtherChannel.

The policer limits the transmission rate of a traffic class and marks actions (conform, exceed, and violate) for each packet. Within the conform, exceed, and violate categories, you decide packet treatments. In the most common configurations, you configure packets that conform to be sent, packets that exceed to be sent with a decreased priority, and packets that violate to be dropped. You can decrease the priority of the CoS, the DSCP, the IP precedence, or the MPLS EXP bits in the packet. You configure the policer by using the `police cir` policy-map class configuration command.

You can also use the `police cir percent` policy-map class configuration command to configure a traffic policer that uses two rates, the CIR and the PIR. The switch calculates the CIR and PIR based on a percentage of the maximum amount of bandwidth assigned to the parent class. The maximum bandwidth is controlled by the `shape` policy-map class configuration command if it is configured. Otherwise, the maximum bandwidth is the physical port bandwidth (1 Gb/s). For more information about the interaction between the `police cir percent` command and the `shape` command, see the `police cir percent` command in the command reference for this release.

Before beginning this procedure, make sure that you have created the class map to isolate traffic. For more information, see the “Classifying Traffic by Using Hierarchical Class Maps” section on page 34-108.

Beginning in privileged EXEC mode, follow these steps to configure a class-level, two-rate traffic policer in a service policy. This procedure is optional. The examples that follow the procedure show how to configure a class-level, a VLAN-level, and a physical-level policer.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>policy-map policy-map-name</td>
<td>Create a policy map by entering the policy-map name, and enter policy-map configuration mode. By default, no policy maps are defined.</td>
</tr>
<tr>
<td>3</td>
<td>class class-name</td>
<td>Specify the name of the class whose traffic policy you want to create or change, and enter policy-map class configuration mode. By default, no traffic classes are defined.</td>
</tr>
</tbody>
</table>
## Configuring Hierarchical QoS

### Step 4

**Command**

```
police cir cir [bc conform-burst] pir pir [be peak-burst] [conform-action action [exceed-action action] [violate-action action]]
```

or

```
police cir percent percent [bc conform-burst ms] [be peak-burst ms] [conform-action action [exceed-action action] [violate-action action]]
```

**Note** For the syntax description of the `police cir percent` command, see the command reference for this release.

**Purpose**

Configure a traffic policer that uses two rates, the CIR and the peak information rate PIR. By default, no policer is defined.

- For `cir cir`, specify the CIR at which the first token bucket is updated. The range is 64000 to 990000000 b/s.
- (Optional) For `bc conform-burst`, specify the conform burst size used by the first token bucket for policing. The range is 1536 to 16776960 bytes. The default is 8192.
- (Optional) For `be peak-burst`, specify the peak burst size used by the second token bucket. The range is 1536 to 16776960 bytes. The default is 8192.
- (Optional) For `be peak-burst`, specify the peak burst size used by the second token bucket. The range is 1536 to 16776960 bytes. The default is 8192.
- (Optional) For `pir pir`, specify the PIR at which the second token bucket for policing is updated. The range is 64000 to 990000000 b/s.
- (Optional) For `conform-action`, specify the action to perform on packets that conform to the CIR and PIR.
- (Optional) For `exceed-action`, specify the action to perform on packets that conform to the PIR but not the CIR.
- (Optional) For `violate-action`, specify the action to perform on packets that exceed the PIR.

**Note** If you do not specify an action, the default `conform-action` is `transmit`, the `exceed-action` is `drop`, and the default `violate-action` is `drop`.

- (Optional) For `action`, specify the action to perform on packets:
  - `drop`—drop the packet.
  - `set-cos-transmit new-cos`—set the CoS value to a new value, and send the packet. The range is 0 to 7.
  - `set-dscp-transmit new-dscp`—set the IP DSCP value to a new value, and send the packet. The range is 0 to 63. You can enter a mnemonic name for a commonly used value.
  - `set-mpls-exp-transmit new-exp`—set the MPLS EXP bits, and send the packet. The range is 0 to 7.
  - `set-prec-transmit new-prec`—set the IP precedence value to a new value, and send the packet. The range is 0 to 7.
  - `transmit`—send the packet without altering it.

If you set the CIR equal to the PIR, a traffic rate that is less than the CIR or that meets the CIR is in the conform range. Traffic that exceeds the CIR rate is in the violate range.

If you set the PIR greater than the CIR, a traffic rate that is less than the CIR is in the conform range. A traffic rate that exceeds the CIR but is less than or equal to the PIR is in the exceed range. A traffic rate that exceeds the PIR is in the violate range.

Setting the burst sizes too low can result in less traffic than expected, and setting them too high can result in more traffic than expected.

### Step 5

**Command**

```
exit
```

**Purpose**

Return to policy-map configuration mode.
To delete an existing policy map, use the `no policy-map policy-map-name` global configuration command. To delete an existing class, use the `no class class-name` policy-map configuration command. To remove the two-rate policer, use the `no police cir [bc conform-burst] pir [be peak-burst] [conform-action action] [exceed-action action] [violate-action action]` policy-map class configuration command. To remove the policy map and interface association, use the `no service-policy output policy-map-name interface configuration command.

This example shows how to configure a class-level, two-rate traffic policer to limit outbound traffic to an average committed rate of 500 kb/s and a peak rate of 1 Mb/s. Traffic marked as conforming to the average committed rate (500 kb/s) is sent as is. Traffic marked as exceeding 500 kb/s, but not exceeding 1 Mb/s, is marked with IP precedence 2 and then sent. All traffic marked as exceeding 1 Mb/s is dropped. The burst parameters are set to 10000 bytes.

```cisco
Switch(config)# class-map c1
Switch(config-cmap)#  match ip precedence 4
Switch(config-cmap)#  exit
Switch(config)#  policy-map policy1
Switch(config-pmap)#  class c1
Switch(config-pmap-c)#  police cir 500000 bc 10000 pir 1000000 be 10000 conform-action transmit exceed-action set-prec-transmit 2 violate-action drop
Switch(config-pmap-c)#  exit
Switch(config)#  interface gigabitethernet1/1
Switch(config-if)#  service-policy output policy1
```

This example shows how to configure a class-level, two-rate traffic policer that uses a CIR and a PIR based on a percentage of bandwidth. A CIR of 20 percent and a PIR of 40 percent are specified. The optional `bc` and `be` values (300 ms and 400 ms, respectively) are specified.

```cisco
Switch(config)# class-map c1
Switch(config-cmap)#  match ip precedence 4
Switch(config-cmap)#  exit
Switch(config)#  policy-map policy1
Switch(config-pmap)#  class class1
Switch(config-pmap-c)#  police cir percent 20 bc 300 ms pir percent 40 be 400 ms
Switch(config-pmap-c)#  exit
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>exit</code></td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td><code>interface interface-id</code></td>
<td>Specify an ES port or an EtherChannel port channel, and enter interface configuration mode.</td>
</tr>
<tr>
<td>`service-policy {input</td>
<td>output} policy-map-name`</td>
</tr>
<tr>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><code>show policy-map policy-map-name</code></td>
<td>Verify your entries.</td>
</tr>
<tr>
<td><code>show policy-map interface interface-id</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
<tr>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

**Note**

If you apply the policy map to an EtherChannel with no ports and then add a standard port to the EtherChannel, the policy is removed from the EtherChannel because standard ports do not support hierarchical QoS.
Switch(config)# interface gigabitethernet1/1/1
Switch(config-if)# service-policy output policy1

This example shows how to configure a VLAN-level, two-rate traffic policer to limit outbound traffic to an average committed rate of 500 kb/s and a peak rate of 1 Mb/s. Traffic marked as conforming to the average committed rate (500 kb/s) is sent as is. Traffic marked as exceeding 500 kb/s, but not exceeding 1 Mb/s, is marked with IP precedence 2 and then sent. All traffic marked as exceeding 1 Mb/s is dropped. The burst parameters are set to 10000 bytes.

Switch(config)# class-map match-all vlan203
Switch(config-cmap)# match vlan 203
Switch(config-cmap)# exit
Switch(config)# policy-map vlan-policy
Switch(config-pmap)# class vlan203
Switch(config-pmap-c)# police cir 500000 bc 10000 pir 1000000 be 10000 conform-action transmit exceed-action set-prec-transmit 2 violate-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit

Switch(config)# interface gigabitethernet1/1/2
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# service-policy output vlan-policy

This example shows how to create a hierarchical service-policy in which all levels are present. This configuration associates a class-level policy map with a VLAN-level policy map, associates the VLAN-level policy map with a physical-level policy map, and attaches the physical-level policy map to a physical port.

Within a policy map, the class- applies to all traffic that is not explicitly matched within the policy map but does match the parent policy. If no parent policy is configured, the parent policy represents the physical port. In a physical-level policy map, class- is the only class that can be configured.

Switch(config)# class-map my-class
Switch(config-cmap)# match ip precedence 1
Switch(config-cmap)# exit
Switch(config)# class-map my-logical-class
Switch(config-cmap)# match vlan 5
Switch(config-cmap)# exit
Switch(config)# policy-map my-class-policy
Switch(config-pmap)# class my-class
Switch(config-pmap-c)# set precedence 2
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# policy-map my-logical-policy
Switch(config-pmap)# class my-logical-class
Switch(config-pmap-c)# service-policy my-class-policy
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# policy-map my-physical-policy
Switch(config-pmap)# class class-
Switch(config-pmap-c)# police cir 500000 bc 10000 pir 1000000 be 10000 conform-action transmit exceed-action set-prec-transmit 2 violate-action drop
Switch(config-pmap-c)# service-policy my-logical-policy
Switch(config-pmap-c)# exit
Switch(config-pmap-c)# exit
Switch(config)# interface gigabitethernet1/1/1
Switch(config)# service-policy input my-physical-policy
This example shows how to configure a class-level, two-rate traffic policer that uses a CIR based on a percentage of bandwidth. A CIR of 5 percent is specified. The switch sets the DSCP value to 16 in packets that conform to the CIR. The port trust state is automatically set to trust CoS.

```
Switch(config)# class-map c1
Switch(config-cmap)# match 1p dscp 8 9 10 11
Switch(config-cmap)# exit
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# police cir percent 5 conform action set-dscp-transmit 16
Switch(config-pmap-c)# exit
Switch(config)# interface gigabitethernet1/1/1
Switch(config-if)# service-policy output policy1
```

### Configuring Class-Based Packet Marking in a Hierarchical Traffic Policy

You can perform class-based packet marking in a hierarchical traffic policy by configuring the `set {cos new-cos | dscp new-dscp | precedence new-precedence | mpls experimental exp-number}` policy-map class configuration command in an policy map attached to an ES port or EtherChannel.

Before beginning this procedure, make sure that you have created the class map to isolate traffic. For more information, see the “Classifying Traffic by Using Hierarchical Class Maps” section on page 34-108.

Beginning in privileged EXEC mode, follow these steps to configure class-level, class-based packet marking in a service policy. This procedure is optional. The examples that follow the procedure show how to configure class-level and VLAN-level class-based packet marking.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>policy-map policy-map-name</strong></td>
</tr>
<tr>
<td></td>
<td>Create a policy map by entering the policy-map name, and enter</td>
</tr>
<tr>
<td></td>
<td>policy-map configuration mode.</td>
</tr>
<tr>
<td></td>
<td>By default, no policy maps are defined.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>class class-name</strong></td>
</tr>
<tr>
<td></td>
<td>Specify the name of the class whose traffic policy you want to create</td>
</tr>
<tr>
<td></td>
<td>or change, and enter policy-map class configuration mode.</td>
</tr>
<tr>
<td></td>
<td>By default, no traffic classes are defined.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>**set {cos new-cos</td>
</tr>
<tr>
<td></td>
<td>Designate the value to set in the traffic class if the packets match the</td>
</tr>
<tr>
<td></td>
<td>criteria.</td>
</tr>
<tr>
<td></td>
<td>• For <strong>cos new-cos</strong>, enter the new CoS value assigned to the</td>
</tr>
<tr>
<td></td>
<td>classified traffic. The range is 0 to 7.</td>
</tr>
<tr>
<td></td>
<td>• For <strong>dscp new-dscp</strong>, enter the new DSCP value assigned to the</td>
</tr>
<tr>
<td></td>
<td>classified traffic. The range is 0 to 63. The specified value sets the</td>
</tr>
<tr>
<td></td>
<td>ToS byte in the packet header.</td>
</tr>
<tr>
<td></td>
<td>• For <strong>precedence new-precedence</strong>, enter the new IP-precedence value</td>
</tr>
<tr>
<td></td>
<td>assigned to the classified traffic. The range is 0 to 7. The specified</td>
</tr>
<tr>
<td></td>
<td>value sets the precedence bit in the IP header.</td>
</tr>
<tr>
<td></td>
<td>• For <strong>mpls experimental exp-number</strong>, enter the new MPLS EXP value</td>
</tr>
<tr>
<td></td>
<td>assigned to the classified traffic. The range is 0 to 7. The specified</td>
</tr>
<tr>
<td></td>
<td>value sets the MPLS EXP 3-bit field in the packet header.</td>
</tr>
</tbody>
</table>
To delete an existing policy map, use the `no policy-map policy-map-name` global configuration command. To delete an existing class, use the `no class class-name` policy-map configuration command. To remove an assigned value, use the `no set {cos new-cos | dscp new-dscp | precedence new-precedence | mpls experimental exp-number}` policy-map class configuration command. To remove the policy map and interface association, use the `no service-policy output policy-map-name` interface configuration command.

**Note**

If you apply the policy map to an EtherChannel with no ports and then add a standard port to the EtherChannel, the policy is removed from the EtherChannel because standard ports do not support hierarchical QoS.

This example shows how to create a class-level policy map called `out_pmap`. When it is attached to the ES port, it matches packets with MPLS EXP field 2 and resets this field to 3.

```
Switch(config)# class-map mpls_2
Switch(config-cmap)# match mpls experimental 2
Switch(config-cmap)# exit
Switch(config)# policy-map out-pmap
Switch(config-pmap)# class mpls_2
Switch(config-pmap-c)# set mpls experimental 3
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config-if)# interface gigabitethernet1/1/1
Switch(config-if)# service-policy output out-pmap
```

This example shows how to create a VLAN-level policy map called `log-policy`. It matches packets with VLAN 203 and associates a class-level child policy called `cls-policy`. The child policy matches packets with MPLS EXP 2 and resets them to 5.

```
Switch(config)# class-map cls-class
Switch(config-cmap)# match mpls experimental 2
Switch(config-cmap)# exit
Switch(config)# class-map log-class
Switch(config-cmap)# match vlan 203
Switch(config-cmap)# exit
Switch(config)# policy-map cls-policy
Switch(config-pmap)# class cls-class
Switch(config-pmap-c)# set mpls experimental 5
```
This example shows how to create a class-level policy map called \textit{p-set}. When it is attached to the ES port, it matches packets with CoS field 4 and resets this field to 3. The port trust state is automatically set to trust CoS.

Switch(config)# class-map c2
Switch(config-cmap)# match cos inner 4
Switch(config-cmap)# exit
Switch(config)# policy-map p-set
Switch(config-pmap)# class c2
Switch(config-pmap-c)# set cos 3
Switch(config-pmap-c)# exit
Switch(config)# interface gigabitethernet1/1/1
Switch(config-if)# service-policy output p-set

### Configuring CBWFQ and Tail Drop

CBWFQ creates a queue for every class for which a class map is defined. Packets satisfying the match criteria for a class accumulate in the queue reserved for the class until they are sent, which occurs when the queue is serviced by the fair queue process. When the maximum packet threshold that you defined for the class is reached, any more packets destined for the class queue are dropped according to the tail drop or WRED mechanism.

You configure tail drop by using the `queue-limit` policy-map class configuration command in a policy map attached to an ES port or EtherChannel. This command configures the maximum threshold for tail drop. Packets are queued until the maximum threshold is exceeded, and then all the packets are dropped.

Before beginning this procedure, make sure that you have reviewed the configuration guidelines and have created the class map to isolate traffic. For more information, see the “Hierarchical QoS Configuration Guidelines” section on page 34-103 and the “Classifying Traffic by Using Hierarchical Class Maps” section on page 34-108. For information on how to configure WRED, see the “Configuring CBWFQ and DSCP-Based WRED” section on page 34-119.

Beginning in privileged EXEC mode, follow these steps to configure class-level CBWFQ and tail drop in a hierarchical service policy. This procedure is optional. The examples that follow the procedure show how to configure class-level and VLAN-level CBWFQ and tail drop.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>policy-map \textit{policy-map-name}</td>
<td>Create a policy map by entering the policy-map name, and enter policy-map configuration mode. By default, no policy maps are defined.</td>
</tr>
</tbody>
</table>
### Configuring Hierarchical QoS

#### Step 3

**Command**: `class class-name`

- **Purpose**: Specify the name of the class whose traffic policy you want to create or change, and enter policy-map class configuration mode.
- By default, no traffic classes are defined.

#### Step 4

**Command**: `bandwidth {bandwidth-kbps | percent percent}`

- **Purpose**: Specify the minimum bandwidth provided to a class belonging to the policy map when there is traffic congestion in the switch. If the switch is not congested, the class receives more bandwidth than you specify with the `bandwidth` command.
- CBWFQ derives the weight for packets belonging to the class from the bandwidth allocated to the class. CBWFQ then uses the weight to ensure that the queue for the class is serviced fairly.
- By default, no bandwidth is specified.

You can specify the bandwidth in kb/s or as a percentage:

- For `bandwidth-kbps`, specify the bandwidth amount in kb/s assigned to the class. The range is 200 to 2000000. Allocate the bandwidth in 100-kb/s increments; otherwise, the software rounds down the bandwidth to the nearest 100-kb/s increment.
- For `percent percent`, specify the percentage of available bandwidth assigned to the class. The range is 1 to 100. The sum of the class bandwidth percentages within a single policy map cannot exceed 99 percent. Percentage calculations are based on the bandwidth available at the parent class (or the physical level if it is the parent).

Specify all the class bandwidths in either kb/s or in percentages, but not a mix of both. The amount of bandwidth configured should be large enough to accommodate Layer 2 overhead.

#### Step 5

**Command**: `queue-limit limit`

- **Purpose**: Configure the maximum threshold for tail drop.
  - For `limit`, the range is 1 to 32768 packets. The default is 128 packets.

#### Step 6

**Command**: `exit`

- **Purpose**: Return to policy-map configuration mode.

#### Step 7

**Command**: `exit`

- **Purpose**: Return to global configuration mode.

#### Step 8

**Command**: `interface interface-id`

- **Purpose**: Specify an ES port or an EtherChannel port channel, and enter interface configuration mode.

#### Step 9

**Command**: `service-policy {input | output} policy-map-name`

- **Purpose**: Specify the policy-map name, and apply it to the ES port or EtherChannel.

#### Step 10

**Command**: `end`

- **Purpose**: Return to privileged EXEC mode.

#### Step 11

**Command**: `show policy-map [policy-map-name [class class-map-name]]`

- **Purpose**: Verify your entries.

  or

**Command**: `show policy-map interface interface-id`

**Purpose**: Verify your entries.

#### Step 12

**Command**: `copy running-config startup-config`

- **Purpose**: (Optional) Save your entries in the configuration file.
To delete an existing policy map, use the `no policy-map policy-map-name` global configuration command. To delete an existing class, use the `no class class-name` policy-map configuration command. To return to the default bandwidth, use the `no bandwidth` policy-map class configuration command. To return to the default maximum threshold, use the `no queue-limit` policy-map class configuration command.

**Note**

If you apply the policy map to an EtherChannel with no ports and then add a standard port to the EtherChannel, the policy is removed from the EtherChannel because standard ports do not support hierarchical QoS.

This example shows how to create a class-level policy map called `policy11` for three classes called `prec1`, `prec2`, and `prec3`. In the policy for these classes, 30 percent of the available bandwidth is assigned to the queue for the first class, 20 percent is assigned to the queue for the second class, and 10 percent is assigned to the queue for the third class. Tail drop is enabled on each class queue, packets are queued until the maximum threshold of 2000 packets is exceeded, and then all the packets are dropped.

```
Switch(config)# class-map prec1
Switch(config-cmap)# match ip precedence 1
Switch(config-cmap)# exit
Switch(config)# class-map prec2
Switch(config-cmap)# match ip precedence 2
Switch(config-cmap)# exit
Switch(config)# class-map prec3
Switch(config-cmap)# match ip precedence 3
Switch(config-cmap)# exit
Switch(config)# policy-map policy11
Switch(config-pmap)# class prec1
Switch(config-pmap-c)# bandwidth percent 30
Switch(config-pmap-c)# queue-limit 2000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class prec2
Switch(config-pmap-c)# bandwidth percent 20
Switch(config-pmap-c)# queue-limit 2000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class prec3
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# queue-limit 2000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet1/1/1
Switch(config-if)# service-policy output policy11
```

This example shows how to create a VLAN-level policy map called `vlan-policy` for two classes called `vlan203` and `vlan202`. In the policy for these classes, the minimum bandwidth is set to 2000 kb/s.

```
Switch(config)# class-map match-all vlan203
Switch(config-cmap)# match vlan 203
Switch(config-cmap)# exit
Switch(config)# class-map match-all vlan202
Switch(config-cmap)# match vlan 202
Switch(config-cmap)# match vlan inner 206
Switch(config-cmap)# exit
Switch(config)# policy-map vlan-policy
Switch(config-pmap)# class vlan203
Switch(config-pmap-c)# bandwidth 2000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class vlan202
Switch(config-pmap-c)# bandwidth 2000
Switch(config-pmap-c)# exit
```
This example shows how to create a VLAN-level policy map called *log-policy*. It matches packets with VLAN 203 and associates a class-level child policy called *cls-policy*. The child policy matches packets with a CoS value of 2, sets 50 percent as the available bandwidth for this class, and sets 2000 packets as the maximum threshold for tail drop. Packets are queued until the maximum threshold is exceeded, and then all the packets are dropped. Note that when you configure the *bandwidth* command in a class policy, you also must configure the *bandwidth* or *shape* policy-map class configuration command in the parent VLAN-level policy.

```
Switch(config)# class-map cls-class
Switch(config-cmap)# match cos 2
Switch(config-cmap)# exit
Switch(config)# class-map log-class
Switch(config-cmap)# match vlan 203
Switch(config-cmap)# exit
Switch(config)# policy-map cls-policy
Switch(config-pmap)# class cls-class
Switch(config-pmap-c)# bandwidth percent 50
Switch(config-pmap-c)# queue-limit 2000
Switch(config-pmap-c)# exit
Switch(config)# policy-map log-policy
Switch(config-pmap)# class log-class
Switch(config-pmap-c)# bandwidth percent 50
Switch(config-pmap-c)# service-policy cls-policy
Switch(config-pmap-c)# exit
Switch(config)# interface gigabitethernet1/1/2
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# service-policy output log-policy
```

### Configuring CBWFQ and DSCP-Based WRED

CBWFQ creates a queue for every class for which a class map is defined. Packets satisfying the match criteria for a class accumulate in the queue reserved for the class until they are sent, which occurs when the queue is serviced by the fair queue process. When the maximum packet threshold that you defined for the class is reached, any more packets destined for the class queue are dropped according to the tail drop or the WRED mechanism.

WRED reduces the chances of tail drop by selectively dropping packets when the port begins to show signs of congestion. By dropping some packets early rather than waiting until the queue is full, WRED avoids dropping large numbers of packets at once.

When a packet arrives and WRED is enabled, these events occur:

- The average queue size is calculate based on the previous average and the current size of the queue. The average queue-size calculation is affected by the exponential weight constant setting in the *random-detect exponential-weight-constant* policy-map class configuration command.

- If the average queue size is less than the minimum queue threshold, the arriving packet is queued. The minimum queue threshold is configured through the *min-threshold* option in the *random-detect dscp* policy-map class configuration command.
If the average queue size is between the minimum queue threshold and the maximum queue threshold, the packet is either dropped or queued, depending on the packet-drop probability. The packet-drop probability is based on the minimum threshold, the maximum threshold, and the mark-probability denominator. The maximum queue threshold is configured through the `max-threshold` option, and the mark-probability denominator is configured through the `mark-prob-denominator` option in the `random-detect dscp` policy-map class configuration command.

If the average queue size is greater than the maximum queue threshold, the packet is automatically dropped.

You enable DSCP-based WRED by using the `random-detect dscp-based` policy-map class configuration command in a policy map attached to an ES port or EtherChannel. This command allows for preferential drop treatment among packets with different DSCP values. The WRED algorithm discards or marks packets destined for a queue when that queue is congested. It discards packets fairly and before the queue is full. If you want to enable IP precedence-based WRED instead of DSCP-based WRED, see the “Configuring CBWFQ and IP Precedence-Based WRED” section on page 34-123.

Before beginning this procedure, make sure that you have reviewed the configuration guidelines and have created the class map to isolate traffic. For more information, see the “Hierarchical QoS Configuration Guidelines” section on page 34-103 and the “Classifying Traffic by Using Hierarchical Class Maps” section on page 34-108. For information on how to configure tail drop, see the “Configuring CBWFQ and Tail Drop” section on page 34-116.

Beginning in privileged EXEC mode, follow these steps to configure class-level CBWFQ and DSCP-based WRED in a hierarchical service policy. This procedure is optional. The examples that follow the procedure show how to configure class-level and VLAN-level CBWFQ and DSCP-based WRED.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>policy-map policy-map-name</code></td>
<td>Create a policy map by entering the policy-map name, and enter</td>
</tr>
<tr>
<td></td>
<td>policy-map configuration mode.</td>
</tr>
<tr>
<td></td>
<td>By default, no policy maps are defined.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>class class-name</code></td>
<td>Specify the name of the class whose traffic policy you want to create</td>
</tr>
<tr>
<td></td>
<td>or change, and enter policy-map class configuration mode.</td>
</tr>
<tr>
<td></td>
<td>By default, no traffic classes are defined.</td>
</tr>
</tbody>
</table>
### Step 4

**Command**

```
bandwidth {bandwidth-kbps \| percent percent}
```

**Purpose**

Specify the minimum bandwidth provided to a class belonging to the policy map when there is traffic congestion in the switch. If the switch is not congested, the class receives more bandwidth than you specify with the `bandwidth` command.

CBWFQ derives the weight for packets belonging to the class from the bandwidth allocated to the class. CBWFQ then uses the weight to ensure that the queue for the class is serviced fairly.

By default, no bandwidth is specified.

You can specify the bandwidth in kb/s or as a percentage:

- For `bandwidth-kbps`, specify the bandwidth amount in kb/s assigned to the class. The range is 200 to 2000000. Allocate the bandwidth in 100-kb/s increments; otherwise, the software rounds down the bandwidth to the nearest 100-kb/s increment.
- For `percent percent`, specify the percentage of available bandwidth assigned to the class. The range is 1 to 100. The sum of the class bandwidth percentages within a single policy map cannot exceed 99 percent. Percentage calculations are based on the bandwidth available at the parent class (or the physical level if it is the parent).

Specify all the class bandwidths in either kb/s or in percentages, but not a mix of both. The amount of bandwidth configured should be large enough to accommodate Layer 2 overhead.

### Step 5

**Command**

```
random-detect dscp-based
```

**Purpose**

Enable DSCP-based WRED as a drop policy. By default, WRED is disabled.

### Step 6

**Command**

```
random-detect dscp dscp min-threshold max-threshold mark-prob-denominator
```

**Purpose**

Specify packet threshold and mark-probability values for a specific DSCP value:

- For `dscp`, enter a DSCP value. The range is 0 to 63. You also can enter a mnemonic name for a commonly used value.
- For `min-threshold`, enter the minimum threshold in packets. The range is 1 to 32768. When the average queue size reaches the minimum threshold, WRED randomly drops some packets with the specified DSCP value.
- For `max-threshold`, enter the maximum threshold in packets. The range is 1 to 32768. The default is 128. When the average queue size exceeds the maximum threshold, WRED drops all packets with the specified DSCP value.
- For `mark-prob-denominator`, enter the denominator for the fraction of packets dropped when the average queue size is at the maximum threshold. The range is 1 to 65535. The default is 10. For example, if the denominator is 512, one out of every 512 packets is dropped when the queue is at the maximum threshold.

For a list of the default settings for a specified DSCP value, see the command reference for this release.
Configuring Hierarchical QoS

### Chapter 34      Configuring QoS

#### Configuring Hierarchical QoS

To delete an existing policy map, use the `no policy-map policy-map-name` global configuration command. To delete an existing class, use the `no class class-name` policy-map configuration command. To return to the default bandwidth, use the `no bandwidth` policy-map class configuration command. To disable DSCP-based WRED, use the `no random-detect dscp-based` policy-map class configuration command. To return to the default WRED settings, use the `no random-detect dscp dscp` policy-map class configuration command.

**Note:** If you apply the policy map to an EtherChannel with no ports and then add a standard port to the EtherChannel, the policy is removed from the EtherChannel because standard ports do not support hierarchical QoS.

This example shows how to configure a class-level policy called `policy10`. Class `c1` has these characteristics: a minimum of 2000 kb/s of bandwidth is expected to be delivered to this class in the event of congestion, and a weight factor of 10 is used to calculate the average queue size. To avoid congestion, DSCP-based WRED packet drop is used instead of tail drop. The minimum threshold for DSCP value 8 is 24, the maximum threshold is 40, and the mark-probability denominator is 512.

```
Switch(config)# class-map c1
Switch(config-cmap)# match ip dscp 8
Switch(config-cmap)# exit
Switch(config)# policy-map policy10
Switch(config-pmap)# class c1
Switch(config-pmap-c)# bandwidth 2000
Switch(config-pmap-c)# random-detect dscp-based
Switch(config-pmap-c)# random-detect exponential-weighting-constant 10
Switch(config-pmap-c)# random-detect dscp 8 24 40 512
Switch(config-pmap-c)# exit
Switch(config)# interface gigabitethernet1/1/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# service-policy output policy10
```

### Command Purpose

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 7</td>
<td><code>random-detect exponential-weighting-constant weight</code></td>
</tr>
<tr>
<td>Step 8</td>
<td><code>exit</code></td>
</tr>
<tr>
<td>Step 9</td>
<td><code>exit</code></td>
</tr>
<tr>
<td>Step 10</td>
<td><code>interface interface-id</code></td>
</tr>
<tr>
<td>Step 11</td>
<td>`service-policy {input</td>
</tr>
<tr>
<td>Step 12</td>
<td><code>end</code></td>
</tr>
<tr>
<td>Step 13</td>
<td><code>show policy-map [policy-map-name [class class-map-name]]</code> or <code>show policy-map interface interface-id</code></td>
</tr>
<tr>
<td>Step 14</td>
<td><code>copy running-config startup-config</code></td>
</tr>
</tbody>
</table>
This example shows how to configure a VLAN-level policy called parent. It matches packets with VLAN 101 and associates a class-level child policy called policy1. The child policy matches two DSCP values in two classes. Thirty percentage of the available bandwidth is assigned to the gold class, 20 percent is assigned to the silver class, and 20 percent is assigned to vlan101. DSCP-based WRED is used as the drop policy. For the af11 value in the gold class, WRED randomly drops packets with this DSCP when the minimum threshold reaches 30. When the average queue size exceeds the maximum threshold of 40, WRED drops all packets with DSCP af11. The mark-probability denominator is set to 10, which means that one out of every 10 packets is dropped when the average queue is at the maximum threshold. The configuration has similar settings for af12 in the gold class and for af21 and af22 in the silver class. Note that when you configure the bandwidth command in a class policy, you also must configure the bandwidth or shape policy-map class configuration command in the parent VLAN-level policy.

Switch(config)# class-map gold
Switch(config-cmap)# match ip dscp af11 af12
Switch(config-cmap)# exit
Switch(config)# class-map silver
Switch(config-cmap)# match ip dscp af21 af22
Switch(config-cmap)# exit
Switch(config)# class-map vlan101
Switch(config-cmap)# match vlan 101
Switch(config-cmap)# exit
Switch(config)# policy-map policy1
Switch(config-pmap)# class gold
Switch(config-pmap-c)# bandwidth percent 30
Switch(config-pmap-c)# random-detect dscp-based
Switch(config-pmap-c)# random-detect dscp af11 30 40 10
Switch(config-pmap-c)# random-detect dscp af12 25 40 10
Switch(config-pmap-c)# exit
Switch(config-pmap)# class silver
Switch(config-pmap-c)# bandwidth percent 20
Switch(config-pmap-c)# random-detect dscp-based
Switch(config-pmap-c)# random-detect dscp af21 28 35 10
Switch(config-pmap-c)# random-detect dscp af22 26 35 10
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# policy-map parent
Switch(config-pmap)# class vlan101
Switch(config-pmap-c)# bandwidth percent 30
Switch(config-pmap-c)# service-policy policy1
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet1/1/1
Switch(config-if)# service-policy output parent

Configuring CBWFQ and IP Precedence-Based WRED

CBWFQ creates a queue for every class for which a class map is defined. Packets satisfying the match criteria for a class accumulate in the queue reserved for the class until they are sent, which occurs when the queue is serviced by the fair queue process. When the maximum packet threshold you defined for the class is reached, any more packets destined for the class queue are dropped according to the tail drop or the WRED mechanism.

WRED reduces the chances of tail drop by selectively dropping packets when the port begins to show signs of congestion. By dropping some packets early rather than waiting until the queue is full, WRED avoids dropping large numbers of packets at once.

You enable IP precedence-based WRED by using the random-detect precedence-based policy-map class configuration command in a policy map attached to an ES port or EtherChannel. This command allows for preferential drop treatment among packets with different IP precedence values. The WRED
algorithm discards or marks packets destined for a queue when that queue is congested. It discards packets fairly and before the queue is full. Packets with high IP-precedence values are preferred over packets with low IP-precedence values. If you want to enable DSCP-based WRED instead of IP precedence-based WRED, see the “Configuring CBWFQ and DSCP-Based WRED” section on page 34-119.

Before beginning this procedure, make sure that you have reviewed the configuration guidelines and have created the class map to isolate traffic. For more information, see the “Hierarchical QoS Configuration Guidelines” section on page 34-103 and the “Classifying Traffic by Using Hierarchical Class Maps” section on page 34-108. For information on how to configure tail drop, see the “Configuring CBWFQ and Tail Drop” section on page 34-116.

Beginning in privileged EXEC mode, follow these steps to configure class-level CBWFQ and IP precedence-based WRED in a hierarchical service policy. This procedure is optional. The examples that follow the procedure show how to configure class-level and VLAN-level CBWFQ and IP precedence-based WRED.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 conﬁgure terminal</td>
<td>Enter global conﬁguration mode.</td>
</tr>
<tr>
<td>Step 2 policy-map policy-map-name</td>
<td>Create a policy map by entering the policy-map name, and enter policy-map conﬁguration mode. By default, no policy maps are deﬁned.</td>
</tr>
<tr>
<td>Step 3 class class-name</td>
<td>Specify the name of the class whose trafﬁc policy you want to create or change, and enter policy-map class conﬁguration mode. By default, no trafﬁc classes are deﬁned.</td>
</tr>
<tr>
<td>Step 4 bandwidth {bandwidth-kbps</td>
<td>percent }</td>
</tr>
<tr>
<td>• For bandwidth-kbps, specify the bandwidth amount in kb/s assigned to the class. The range is 200 to 2000000. Allocate the bandwidth in 100-kb/s increments; otherwise, the software rounds down the bandwidth to the nearest 100-kb/s increment.</td>
<td></td>
</tr>
<tr>
<td>• For percent percent, specify the percentage of available bandwidth assigned to the class. The range is 1 to 100. The sum of the class bandwidth percentages within a single policy map cannot exceed 99 percent. Percentage calculations are based on the bandwidth available at the parent class (or the physical level if it is the parent).</td>
<td></td>
</tr>
</tbody>
</table>

Specify all the class bandwidths in either kb/s or in percentages, but not a mix of both. The amount of bandwidth conﬁgured should be large enough to accommodate Layer 2 overhead.
Step 5  
**random-detect precedence-based**  
Enable IP precedence-based WRED as a drop policy. By default, WRED is disabled.

Step 6  
**random-detect precedence ip-precedence min-threshold max-threshold mark-prob-denominator**  
Specify packet threshold and mark-probability values for a specific IP precedence value:  
- For **ip-precedence**, specify an IP precedence value. The range is 0 to 7.  
- For **min-threshold**, specify the minimum threshold in packets. The range is 1 to 32768. When the average queue size reaches the minimum threshold, WRED randomly drops some packets with the specified precedence value.  
- For **max-threshold**, specify the maximum threshold in packets. The range is 1 to 32768. When the average queue size exceeds the maximum threshold, WRED drops all packets with the specified precedence value.  
- For **mark-prob-denominator**, specify the denominator for the fraction of packets dropped when the average queue size is at the maximum threshold. The range is 1 to 65535. The default is 10. For example, if the denominator is 512, one out of every 512 packets is dropped when the queue is at the maximum threshold.

For a list of the default settings for a specified IP precedence value, see the command reference for this release.

Step 7  
**random-detect exponential-weighting-constant weight**  
(Optional) Configure the exponential weight factor for the average queue-size calculation for WRED. The range is 1 to 16. The default is 9.

Step 8  
**exit**  
Return to policy-map configuration mode.

Step 9  
**exit**  
Return to global configuration mode.

Step 10  
**interface interface-id**  
Specify an ES port or an EtherChannel port channel, and enter interface configuration mode.

Step 11  
**service-policy [input | output] policy-map-name**  
Specify the policy-map name, and apply it to the ES port or EtherChannel.

Step 12  
**end**  
Return to privileged EXEC mode.

Step 13  
**show policy-map [policy-map-name [class class-map-name]]**  
or  
**show policy-map interface interface-id**  
Verify your entries.

Step 14  
**copy running-config startup-config**  
(Optional) Save your entries in the configuration file.

To delete an existing policy map, use the **no policy-map policy-map-name** global configuration command. To delete an existing class, use the **no class class-name** policy-map configuration command. To return to the default bandwidth, use the **no bandwidth** policy-map class configuration command. To disable IP precedence-based WRED, use the **no random-detect precedence-based** policy-map class configuration command. To return to the default WRED settings, use the **no random-detect precedence ip-precedence** policy-map class configuration command.
Chapter 34  Configuring QoS

Configuring Hierarchical QoS

If you apply the policy map to an EtherChannel with no ports and then add a standard port to the EtherChannel, the policy is removed from the EtherChannel because standard ports do not support hierarchical QoS.

This example shows how to configure a class-level policy called policy10. Class c1 has these characteristics: a minimum of 2000 kb/s of bandwidth is expected to be delivered to this class in the event of congestion, and a weight factor of 10 is used to calculate the average queue size. To avoid congestion, WRED packet drop is used instead of tail drop. IP precedence is reset for levels 0 to 2. The minimum threshold for IP precedence value 0 is 32, the maximum threshold is 256, and the mark-probability denominator is 100. IP precedence values 1 and 2 have similar thresholds and probability denominators.

```
Switch(config)# class-map c1
Switch(config-cmap)# match ip precedence 0 1 2
Switch(config-cmap)# exit
Switch(config)# policy-map policy10
Switch(config-pmap)# class c1
Switch(config-pmap-c)# bandwidth 2000
Switch(config-pmap-c)# random-detect precedence-based
Switch(config-pmap-c)# random-detect exponential-weighting-constant 10
Switch(config-pmap-c)# random-detect precedence 0 32 256 100
Switch(config-pmap-c)# random-detect precedence 1 64 256 100
Switch(config-pmap-c)# random-detect precedence 2 96 256 100
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet1/1/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# service-policy output policy10
```

This example shows how to configure a VLAN-level policy called parent. It matches packets with VLAN 101 and associates a class-level child policy called policy1. The child policy matches two IP precedence values in two classes. Thirty percentage of the available bandwidth is assigned to the gold class, 20 percent is assigned to the silver class, and 30 percent is assigned to vlan101. IP precedence-based WRED is used as the drop policy. For the IP precedence 0 in the gold class, WRED randomly drops packets with this IP precedence when the minimum threshold reaches 30. When the average queue size exceeds the maximum threshold of 40, WRED drops all packets with IP precedence 0. The mark-probability denominator is set to 10, which means that one out of every 10 packets is dropped when the average queue is at the maximum threshold. The configuration has similar settings for IP precedence 3 in the silver class. Note that when you configure the bandwidth command in a class policy, you also must configure the bandwidth or shape policy-map class configuration command in the parent VLAN-level policy.

```
Switch(config)# class-map gold
Switch(config-cmap)# match ip precedence 0
Switch(config-cmap)# exit
Switch(config)# class-map silver
Switch(config-cmap)# match ip precedence 3
Switch(config-cmap)# exit
Switch(config)# class-map vlan101
Switch(config-cmap)# match vlan 101
Switch(config-cmap)# exit
Switch(config)# policy-map policy1
Switch(config-pmap)# class gold
Switch(config-pmap-c)# bandwidth percent 30
Switch(config-pmap-c)# random-detect precedence-based
Switch(config-pmap-c)# random-detect precedence 0 30 40 10
Switch(config-pmap-c)# exit
Switch(config-pmap-c)# class silver
```
Enabling LLQ

LLQ provides strict-priority queueing for a traffic class. It enables delay-sensitive data, such as voice, to be sent before packets in other queues are sent. The priority queue is serviced first until it is empty. Only one traffic stream can be destined for the priority queue per class-level policy. The priority queue restricts all traffic streams in the same hierarchy, and you should use care when configuring this feature. You enable the priority queue for a traffic class by using the `priority` policy-map class configuration command in a policy map attached to an ES port or EtherChannel.

To avoid losing priority traffic on an ES port when the switch is congested, you can use both strict-priority queueing and egress priority queueing. Note that when you map certain traffic classes to the egress priority queue, they are not automatically placed into the strict-priority queue. You must enter both the `priority` policy-map class configuration and the `priority-queue out` interface configuration commands. For more information, see the “Configuring the Egress Priority Queue” section on page 34-97.

Before beginning this procedure, make sure that you have reviewed the configuration guidelines and have created the class map to isolate traffic. For more information, see the “Hierarchical QoS Configuration Guidelines” section on page 34-103 and the “Classifying Traffic by Using Hierarchical Class Maps” section on page 34-108.

Beginning in privileged EXEC mode, follow these steps to enable class-level priority queueing in a hierarchical service policy. This procedure is optional. The examples that follow the procedure show how to enable class-level and VLAN-level priority queueing.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 policy-map policy-map-name</td>
<td>Create a policy map by entering the policy-map name, and enter policy-map configuration mode. By default, no policy maps are defined.</td>
</tr>
<tr>
<td>Step 3 class class-name</td>
<td>Specify the name of the class whose traffic policy you want to create or change, and enter policy-map class configuration mode. By default, no traffic classes are defined.</td>
</tr>
<tr>
<td>Step 4 priority</td>
<td>Enable the strict-priority queue, and give priority to a class of traffic. By default, strict-priority queueing is disabled.</td>
</tr>
<tr>
<td>Step 5 exit</td>
<td>Return to policy-map configuration mode.</td>
</tr>
</tbody>
</table>
To delete an existing policy map, use the `no policy-map policy-map-name` global configuration command. To delete an existing class, use the `no class class-name` policy-map configuration command. To disable the priority queue, use the `no priority policy-map class configuration` command.

This example shows how to configure a class-level policy called `policy1` that has two classes. Class 1 has 10 percent of the available bandwidth. Class 2 is configured as the priority queue, which is serviced first until it is empty.

```plaintext
Switch(config)# class-map class1
Switch(config-cmap)# match mpls experimental 2 3 4
Switch(config-cmap)# exit
Switch(config)# class-map class2
Switch(config-cmap)# match mpls experimental 7
Switch(config-cmap)# exit
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class2
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet1/1/2
Switch(config-if)# service-policy output policy1
```

This example shows how to configure a VLAN-level policy called `parent`. It matches packets with VLAN 101 and associates a class-level child policy called `policy1`. The gold class is configured as the priority queue, whereas the silver class and vlan101 class each have 20 percent of the available bandwidth assigned to them. DSCP-based WRED is used as the drop policy. For the af21 value in the silver class, WRED randomly drops packets with this DSCP when the minimum threshold reaches 28. When the average queue size exceeds the maximum threshold of 35, WRED drops all packets with DSCP af21. The mark-probability denominator is set to 10, which means that one out of every 10 packets is dropped when the average queue is at the maximum threshold. The configuration has similar settings for af22 in the silver class.

```plaintext
Switch(config)# class-map gold
Switch(config-cmap)# match ip dscp af11 af12
Switch(config-cmap)# exit
Switch(config)# class-map silver
Switch(config-cmap)# match ip dscp af21 af22
Switch(config-cmap)# exit
Switch(config)# class-map vlan101
```
Switch(config-cmap)# match vlan 101
Switch(config-cmap)# exit
Switch(config)# policy-map policy1
Switch(config-pmap)# class gold
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# exit
Switch(config-pmap)# class silver
Switch(config-pmap-c)# bandwidth percent 20
Switch(config-pmap-c)# random-detect dscp-based
Switch(config-pmap-c)# random-detect dscp af21 28 35 10
Switch(config-pmap-c)# random-detect dscp af22 26 35 10
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# policy-map parent
Switch(config-pmap)# class vlan101
Switch(config-pmap-c)# bandwidth percent 20
Switch(config-pmap-c)# service-policy policy1
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet1/1/1
Switch(config-if)# service-policy output parent

Configuring Shaping

Shaping provides a process for delaying out-of-profile packets in queues so that they conform to a specified profile. Shaping is distinct from policing. Policing drops packets that exceed a configured threshold, but shaping buffers packets so that traffic remains within a threshold. Shaping offers greater smoothness in handling traffic than policing. You can configure average-rate traffic shaping on a traffic class within a policy map at the class level, at the VLAN level, and at the physical level by using the `shape` policy-map class configuration command. At the physical level of the hierarchy, you can shape only the class- class in a policy attached to an ES port or EtherChannel.

Before beginning this procedure, make sure that you have reviewed the configuration guidelines and have created the class map to isolate traffic. For more information, see the “Hierarchical QoS Configuration Guidelines” section on page 34-103 and the “Classifying Traffic by Using Hierarchical Class Maps” section on page 34-108.

Beginning in privileged EXEC mode, follow these steps to configure class-level shaping in a hierarchical service policy. This procedure is optional. The examples that follow the procedure show how to configure class-level, VLAN-level, and physical-level shaping.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 policy-map <code>policy-map-name</code></td>
<td>Create a policy map by entering the policy-map name, and enter policy-map configuration mode. By default, no policy maps are defined.</td>
</tr>
<tr>
<td>Step 3 class <code>class-name</code></td>
<td>Specify the name of the class whose traffic policy you want to create or change, and enter policy-map class configuration mode. By default, no traffic classes are defined.</td>
</tr>
</tbody>
</table>
To delete an existing policy map, use the `no policy-map policy-map-name` global configuration command. To delete an existing class, use the `no class class-name` policy-map configuration command. To disable the average-rate traffic shaping, use the `no shape average` policy-map class configuration command.

This example shows how to configure class-level, average-rate shaping. It limits traffic class `class1` to a data transmission rate of 256 kb/s.

```bash
Switch(config)# class-map class1
Switch(config-cmap)# match cos 0 1 2 3
Switch(config-cmap)# exit
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# shape average 256000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet1/1/1
Switch(config-if)# service-policy output policy1
```

This example shows how to configure VLAN-level, average-rate shaping. It limits each traffic class, `vlan101` and `vlan102`, to a data transmission rate of 400 Mb/s.

```bash
Switch(config)# class-map match-all vlan101
Switch(config-cmap)# match vlan 101
Switch(config-cmap)# exit
Switch(config)# class-map match-all vlan102
Switch(config-cmap)# match vlan 102
Switch(config-cmap)# exit
Switch(config)# policy-map vlan-policy
```
Switch(config-pmap)# class vlan101
Switch(config-pmap-c)# shape average 400000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class vlan102
Switch(config-pmap-c)# shape average 400000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet1/1/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# service-policy output vlan-policy

This example shows how to shape the class. This configuration associates a class-level policy map with a VLAN-level policy map and then associates the VLAN-level policy map with a physical-level policy map.

Switch(config)# class-map my-class
Switch(config-cmap)# match ip precedence 1
Switch(config-cmap)# exit
Switch(config)# class-map my-logical-class
Switch(config-cmap)# match vlan 5
Switch(config-cmap)# exit
Switch(config)# policy-map my-class-policy
Switch(config-pmap)# class my-class
Switch(config-pmap-c)# set precedence 2
Switch(config-pmap-c)# exit
Switch(config)# policy-map my-logical-policy
Switch(config-pmap)# class my-logical-class
Switch(config-pmap-c)# shape average 400000000
Switch(config-pmap-c)# service-policy my-class-policy
Switch(config-pmap-c)# exit
Switch(config)# policy-map my-physical-policy
Switch(config-pmap)# class class-
Switch(config-pmap-c)# shape average 500000000
Switch(config-pmap-c)# service-policy my-logical-policy

Displaying Hierarchical QoS Information

To display hierarchical QoS information, use one or more of the privileged EXEC commands in Table 34-17:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show class-map [class-map-name]</td>
<td>Display QoS class maps, which define the match criteria to classify traffic.</td>
</tr>
<tr>
<td>show mls qos</td>
<td>Display global QoS configuration information.</td>
</tr>
<tr>
<td>show policy-map [policy-map-name [class class-map-name]]</td>
<td>Display QoS policy maps, which define the traffic policy for a traffic class.</td>
</tr>
<tr>
<td>show policy-map interface interface-id output [class class-name]]</td>
<td>Display QoS policy-map information for the specified ES port, and display statistics for an individual class.</td>
</tr>
</tbody>
</table>
Configuring EtherChannels and Link-State Tracking

This chapter describes how to configure EtherChannels on Layer 2 and Layer 3 ports on the Catalyst 3750 Metro switch. EtherChannel provides fault-tolerant high-speed links between switches, routers, and servers. You can use it to increase the bandwidth between the wiring closets and the data center, and you can deploy it anywhere in the network where bottlenecks are likely to occur. EtherChannel provides automatic recovery for the loss of a link by redistributing the load across the remaining links. If a link fails, EtherChannel redirects traffic from the failed link to the remaining links in the channel without intervention.

This chapter also describes how to configure link-state tracking.

Note: For complete syntax and usage information for the commands used in this chapter, see the command reference for this release.

This chapter consists of these sections:

- Understanding EtherChannels, page 35-1
- Configuring EtherChannels, page 35-8
- Displaying EtherChannel, PAgP, and LACP Status, page 35-20
- Understanding Link-State Tracking, page 35-21
- Configuring Link-State Tracking, page 35-22

Understanding EtherChannels

These sections describe how EtherChannels work:

- EtherChannel Overview, page 35-2
- Port-Channel Interfaces, page 35-3
- Port Aggregation Protocol, page 35-4
- Link Aggregation Control Protocol, page 35-5
- EtherChannel On Mode, page 35-6
- Load Balancing and Forwarding Methods, page 35-6
Understanding EtherChannels

EtherChannel Overview

An EtherChannel consists of individual Fast Ethernet or Gigabit Ethernet links bundled into a single logical link as shown in Figure 35-1.

![Figure 35-1 Typical EtherChannel Configuration](image)

The EtherChannel provides full-duplex bandwidth up to 800 Mbps (Fast EtherChannel) or 2 Gbps (Gigabit EtherChannel) between your switch and another switch or host. You cannot bundle standard Gigabit Ethernet ports with the enhanced-services (ES) Gigabit Ethernet ports.

Each EtherChannel can consist of up to eight compatibly configured Ethernet ports. All ports in each EtherChannel must be configured as either Layer 2 or Layer 3 ports. For Catalyst 3750 Metro switches, the number of EtherChannels is limited to 12. For more information, see the “EtherChannel Configuration Guidelines” section on page 35-9. The EtherChannel Layer 3 ports are made up of routed ports. Routed ports are physical ports configured to be in Layer 3 mode by using the `no switchport` interface configuration command. For more information, see the Chapter 9, “Configuring Interface Characteristics.”

You can configure an EtherChannel in one of these modes: Port Aggregation Protocol (PAgP), Link Aggregation Control Protocol (LACP), or On mode. Configure both ends of the EtherChannel in the same mode:

- When you configure one end of an EtherChannel in either PAgP or LACP mode, the system negotiates with the other end of the channel to determine which ports should become active. Incompatible ports are suspended.
- When you configure an EtherChannel in the on mode, no negotiations take place. The switch forces all compatible ports to become active in the EtherChannel. The other end of the channel (on the other switch) must also be configured in the on mode; otherwise, packet loss can occur.
Beginning with Cisco IOS Release 12.2(35)SE, instead of a suspended state, the local port is put into an independent state and continues to carry data traffic as would any other single link. The port configuration does not change, but the port does not participate in the EtherChannel.

If a link within an EtherChannel fails, traffic previously carried over that failed link moves to the remaining links within the EtherChannel. If traps are enabled on the switch, a trap is sent for a failure that identifies the switch, the EtherChannel, and the failed link. Inbound broadcast and multicast packets on one link in an EtherChannel are blocked from returning on any other link of the EtherChannel.

### Port-Channel Interfaces

When you create an EtherChannel, a port-channel logical interface is involved:

- With Layer 2 ports, use the `channel-group` interface configuration command to dynamically create the port-channel logical interface.

  You also can use the `interface port-channel port-channel-number` global configuration command to manually create the port-channel logical interface, but then you must use the `channel-group channel-group-number` command to bind the logical interface to a physical port. The `channel-group-number` can be the same as the `port-channel-number`, or you can use a new number. If you use a new number, the `channel-group` command dynamically creates a new port channel.

- With Layer 3 ports, you should manually create the logical interface by using the `interface port-channel` global configuration command followed by the `no switchport` interface configuration command. Then you manually assign an interface to the EtherChannel by using the `channel-group` interface configuration command.

For both Layer 2 and Layer 3 ports, the `channel-group` command binds the physical port and the logical interface together as shown in Figure 35-2.

Each EtherChannel has a port-channel logical interface numbered from 1 to 12. This port-channel interface number corresponds to the one specified with the `channel-group` interface configuration command.

**Figure 35-2 Relationship of Physical Ports, Logical Port Channels, and Channel Groups**
After you configure an EtherChannel, configuration changes applied to the port-channel apply to all the physical ports assigned to the port-channel. Configuration changes applied to the physical port affect only the port where you apply the configuration. To change the parameters of all ports in an EtherChannel, apply configuration commands to the port-channel interface, for example, spanning-tree commands or commands to configure a Layer 2 EtherChannel as a trunk.

### Port Aggregation Protocol

The Port Aggregation Protocol (PAgP) is a Cisco-proprietary protocol that can be run only on Cisco switches and on those switches licensed by vendors to support PAgP. PAgP facilitates the automatic creation of EtherChannels by exchanging PAgP packets between Ethernet ports.

By using PAgP, the switch learns the identity of partners capable of supporting PAgP and the capabilities of each port. It then dynamically groups similarly configured ports into a single logical link (channel or aggregate port). Similarly configured ports are grouped based on hardware, administrative, and port parameter constraints. For example, PAgP groups the ports with the same speed, duplex mode, native VLAN, VLAN range, and trunking status and type. After grouping the links into an EtherChannel, PAgP adds the group to the spanning tree as a single switch port.

### PAgP Modes

Table 35-1 shows the user-configurable EtherChannel PAgP modes for the channel-group interface configuration command.

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto</td>
<td>Places a port into a passive negotiating state, in which the port responds to PAgP packets it receives but does not start PAgP packet negotiation. This setting minimizes the transmission of PAgP packets.</td>
</tr>
<tr>
<td>desirable</td>
<td>Places a port into an active negotiating state, in which the port starts negotiations with other ports by sending PAgP packets.</td>
</tr>
</tbody>
</table>

Switch ports exchange PAgP packets only with partner ports configured in the auto or desirable modes. Ports configured in the on mode do not exchange PAgP packets.

Both the auto and desirable modes enable ports to negotiate with partner ports to form an EtherChannel based on criteria such as port speed and, for Layer 2 EtherChannels, trunking state and VLAN numbers.

Ports can form an EtherChannel when they are in different PAgP modes as long as the modes are compatible. For example:

- A port in the desirable mode can form an EtherChannel with another port that is in the desirable or auto mode.
- A port in the auto mode can form an EtherChannel with another port in the desirable mode.

A port in the auto mode cannot form an EtherChannel with another port that is also in the auto mode because neither port starts PAgP negotiation.

If your switch is connected to a partner that is PAgP-capable, you can configure the switch port for nonsilent operation by using the non-silent keyword. If you do not specify non-silent with the auto or desirable mode, silent mode is assumed.
Use the silent mode when the switch is connected to a device that is not PAgP-capable and seldom, if ever, sends packets. An example of a silent partner is a file server or a packet analyzer that is not generating traffic. In this case, running PAgP on a physical port connected to a silent partner prevents that switch port from ever becoming operational. However, the silent setting allows PAgP to operate, to attach the port to a channel group, and to use the port for transmission.

**PAgP Interaction with Other Features**

The Dynamic Trunking Protocol (DTP) and the Cisco Discovery Protocol (CDP) send and receive packets over the physical ports in the EtherChannel. Trunk ports send and receive PAgP protocol data units (PDUs) on the lowest numbered VLAN.

In Layer 2 EtherChannels, the first port in the channel that comes up provides its MAC address to the EtherChannel. If this port is removed from the bundle, one of the remaining ports in the bundle provides its MAC address to the EtherChannel.

PAgP sends and receives PAgP PDUs only from ports that are up and have PAgP enabled for the auto or desirable mode.

**Link Aggregation Control Protocol**

The LACP is defined in IEEE 802.3ad and enables Cisco switches to manage Ethernet channels between switches that conform to the 802.3ad protocol. LACP facilitates the automatic creation of EtherChannels by exchanging LACP packets between Ethernet ports.

By using LACP, the switch learns the identity of partners capable of supporting LACP and the capabilities of each port. It then dynamically groups similarly configured ports into a single logical link (channel or aggregate port). Similarly configured ports are grouped based on hardware, administrative, and port parameter constraints. For example, LACP groups the ports with the same speed, duplex mode, native VLAN, VLAN range, and trunking status and type. After grouping the links into an EtherChannel, LACP adds the group to the spanning tree as a single switch port.

**LACP Modes**

Table 35-2 shows the user-configurable EtherChannel LACP modes for the `channel-group` interface configuration command.

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>active</td>
<td>Places a port into an active negotiating state in which the port starts negotiations with other ports by sending LACP packets.</td>
</tr>
<tr>
<td>passive</td>
<td>Places a port into a passive negotiating state in which the port responds to LACP packets that it receives, but does not start LACP packet negotiation. This setting minimizes the transmission of LACP packets.</td>
</tr>
</tbody>
</table>

Both the active and passive LACP modes enable ports to negotiate with partner ports to form an EtherChannel based on criteria such as port speed and, for Layer 2 EtherChannels, trunking state and VLAN numbers.
Understanding EtherChannels

Ports can form an EtherChannel when they are in different LACP modes as long as the modes are compatible. For example:

- A port in the **active** mode can form an EtherChannel with another port that is in the **active** or **passive** mode.
- A port in the **passive** mode cannot form an EtherChannel with another port that is also in the **passive** mode because neither port starts LACP negotiation.

**LACP Interaction with Other Features**

The DTP and the CDP send and receive packets over the physical ports in the EtherChannel. Trunk ports send and receive LACP PDUs on the lowest numbered VLAN.

In Layer 2 EtherChannels, the first port in the channel that comes up provides its MAC address to the EtherChannel. If this port is removed from the bundle, one of the remaining ports in the bundle provides its MAC address to the EtherChannel.

LACP sends and receives LACP PDUs only from ports that are up and have LACP enabled for the active or passive mode.

**EtherChannel On Mode**

EtherChannel on mode can be used to manually configure an EtherChannel. The on mode forces a port to join an EtherChannel without negotiations. The on mode can be useful if the remote device does not support PAgP or LACP. In the on mode, a usable EtherChannel exists only when the switches at both ends of the link are configured in the on mode.

Ports that are configured in the on mode in the same channel group must have compatible port characteristics, such as speed and duplex. Ports that are not compatible are suspended, even though they are configured in the on mode.

**Caution**

You should use care when using the on mode. This is a manual configuration, and ports on both ends of the EtherChannel must have the same configuration. If the group is misconfigured, packet loss or spanning-tree loops can occur.

**Load Balancing and Forwarding Methods**

EtherChannel balances the traffic load across the links in a channel by reducing part of the binary pattern formed from the addresses in the frame to a numerical value that selects one of the links in the channel. EtherChannel load balancing can use MAC addresses or IP addresses, source or destination addresses, or both source and destination addresses. The selected mode applies to all EtherChannels configured on the switch. You configure the load balancing and forwarding method by using the **port-channel load-balance** global configuration command.

With source-MAC address forwarding, when packets are forwarded to an EtherChannel, they are distributed across the ports in the channel based on the source-MAC address of the incoming packet. Therefore, to provide load balancing, packets from different hosts use different ports in the channel, but packets from the same host use the same port in the channel.
With destination-MAC address forwarding, when packets are forwarded to an EtherChannel, they are distributed across the ports in the channel based on the destination host’s MAC address of the incoming packet. Therefore, packets to the same destination are forwarded over the same port, and packets to a different destination are sent on a different port in the channel.

With source-and-destination MAC address forwarding, when packets are forwarded to an EtherChannel, they are distributed across the ports in the channel based on both the source and destination MAC addresses. This forwarding method, a combination source-MAC and destination-MAC address forwarding methods of load distribution, can be used if it is not clear whether source-MAC or destination-MAC address forwarding is better suited on a particular switch. With source-and-destination MAC-address forwarding, packets sent from host A to host B, host A to host C, and host C to host B could all use different ports in the channel.

With source-IP address-based forwarding, when packets are forwarded to an EtherChannel, they are distributed across the ports in the EtherChannel based on the source-IP address of the incoming packet. Therefore, to provide load-balancing, packets from different IP addresses use different ports in the channel, but packets from the same IP address use the same port in the channel.

With destination-IP address-based forwarding, when packets are forwarded to an EtherChannel, they are distributed across the ports in the EtherChannel based on the destination-IP address of the incoming packet. Therefore, to provide load-balancing, packets from the same IP source address sent to different IP destination addresses could be sent on different ports in the channel. But packets sent from different source IP addresses to the same destination IP address are always sent on the same port in the channel.

With source-and-destination IP address-based forwarding, when packets are forwarded to an EtherChannel, they are distributed across the ports in the EtherChannel based on both the source and destination IP addresses of the incoming packet. This forwarding method, a combination of source-IP and destination-IP address-based forwarding, can be used if it is not clear whether source-IP or destination-IP address-based forwarding is better suited on a particular switch. In this method, packets sent from the IP address A to IP address B, from IP address A to IP address C, and from IP address C to IP address B could all use different ports in the channel.

Different load-balancing methods have different advantages, and the choice of a particular load-balancing method should be based on the position of the switch in the network and the kind of traffic that needs to be load-distributed. In Figure 35-3, an EtherChannel of four workstations communicates with a router. Because the router is a single-MAC-address device, source-based forwarding on the switch EtherChannel ensures that the switch uses all available bandwidth to the router. The router is configured for destination-based forwarding because the large number of workstations ensures that the traffic is evenly distributed from the router EtherChannel.

Use the option that provides the greatest variety in your configuration. For example, if the traffic on a channel is going only to a single MAC address, using the destination-MAC address always chooses the same link in the channel. Using source addresses or IP addresses might result in better load balancing.
Figure 35-3 Load Distribution and Forwarding Methods

Configuring EtherChannels

These sections describe how to configure EtherChannel on Layer 2 and Layer 3 ports:

- Default EtherChannel Configuration, page 35-9
- EtherChannel Configuration Guidelines, page 35-9
- Configuring Layer 2 EtherChannels, page 35-10 (required)
- Configuring Layer 3 EtherChannels, page 35-13 (required)
- Configuring EtherChannel Load Balancing, page 35-16 (optional)
- Configuring the PAgP Learn Method and Priority, page 35-17 (optional)
- Configuring LACP Hot-Standby Ports, page 35-18 (optional)

**Note**
Make sure that the ports are correctly configured. For more information, see the “EtherChannel Configuration Guidelines” section on page 35-9.

**Note**
After you configure an EtherChannel, configuration changes applied to the port-channel interface apply to all the physical ports assigned to the port-channel interface, and configuration changes applied to the physical port affect only the port where you apply the configuration.
Default EtherChannel Configuration

Table 35-3 shows the default EtherChannel configuration.

Table 35-3 Default EtherChannel Configuration

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channel groups</td>
<td>None assigned.</td>
</tr>
<tr>
<td>Port-channel logical interface</td>
<td>None defined.</td>
</tr>
<tr>
<td>PAgP mode</td>
<td>No default.</td>
</tr>
<tr>
<td>PAgP learn method</td>
<td>Aggregate-port learning on all ports.</td>
</tr>
<tr>
<td>PAgP priority</td>
<td>128 on all ports.</td>
</tr>
<tr>
<td>LACP mode</td>
<td>No default.</td>
</tr>
<tr>
<td>LACP learn method</td>
<td>Aggregate-port learning on all ports.</td>
</tr>
<tr>
<td>LACP port priority</td>
<td>32768 on all ports.</td>
</tr>
<tr>
<td>LACP system priority</td>
<td>32768.</td>
</tr>
<tr>
<td>LACP system ID</td>
<td>LACP system priority and the switch MAC address.</td>
</tr>
<tr>
<td>Load balancing</td>
<td>Load distribution on the switch is based on the source-MAC address of the incoming packet.</td>
</tr>
</tbody>
</table>

EtherChannel Configuration Guidelines

If improperly configured, some EtherChannel ports are automatically disabled to avoid network loops and other problems. Follow these guidelines to avoid configuration problems:

- More than 12 EtherChannels cannot be configured on the switch.
- Do not bundle standard Gigabit Ethernet ports with the enhanced-services (ES) Gigabit Ethernet ports.
- Configure a PAgP EtherChannel with up to eight Ethernet ports of the same type.
- Configure a LACP EtherChannel with up to 16 Ethernet ports of the same type. Up to eight ports can be active, and up to eight ports can be in standby mode.
- Configure all ports in an EtherChannel to operate at the same speeds and duplex modes.
- Enable all ports in an EtherChannel. A port in an EtherChannel that is disabled by using the `shutdown` interface configuration command is treated as a link failure, and its traffic is transferred to one of the remaining ports in the EtherChannel.
- 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 these parameters, you must also make the changes to all ports in the group:
  - Allowed-VLAN list
  - Spanning-tree path cost for each VLAN
  - Spanning-tree port priority for each VLAN
  - Spanning-tree Port Fast setting
• Do not configure a port to be a member of more than one EtherChannel group.
• Do not enable link-state tracking on individual interfaces that will be part of a downstream Etherchannel interface.
• Do not configure an EtherChannel in both the PAgP and LACP modes. EtherChannel groups running PAgP and LACP can coexist on the same switch. Individual EtherChannel groups can run either PAgP or LACP, but they cannot interoperate.
• Do not configure a Switched Port Analyzer (SPAN) destination as part of an EtherChannel.
• Do not configure a secure port as part of an EtherChannel or the reverse.
• Do not configure a private-VLAN port as part of an EtherChannel.
• Do not configure a port that is an active member of an EtherChannel as an 802.1x port. If 802.1x is enabled on a not-yet active port of an EtherChannel, the port does not join the EtherChannel.

Note
In software releases earlier than Cisco IOS Release 12.2(25)EY, if 802.1x is enabled on a not-yet-active port of an EtherChannel, the port does not join the EtherChannel.

• For Layer 2 EtherChannels:
  – Assign all ports in the EtherChannel to the same VLAN, or configure them as trunks. Ports with different native VLANs cannot form an EtherChannel.
  – If you configure an EtherChannel from trunk ports, verify that the trunking mode (ISL or 802.1Q) is the same on all the trunks. Inconsistent trunk modes on EtherChannel ports can have unexpected results.
  – An EtherChannel supports the same allowed range of VLANs on all the ports in a trunking Layer 2 EtherChannel. If the allowed range of VLANs is not the same, the ports do not form an EtherChannel even when PAgP is set to the auto or desirable mode.
  – Ports with different spanning-tree path costs can form an EtherChannel if they are otherwise compatibly configured. Setting different spanning-tree path costs does not, by itself, make ports incompatible for the formation of an EtherChannel.
• For Layer 3 EtherChannels, assign the Layer 3 address to the port-channel logical interface, not to the physical ports in the channel.

Configuring Layer 2 EtherChannels

You configure Layer 2 EtherChannels by assigning ports to a channel group with the channel-group interface configuration command. This command automatically creates the port-channel logical interface.
Beginning in privileged EXEC mode, follow these steps to assign a Layer 2 Ethernet port to a Layer 2 EtherChannel. This procedure is required.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>interface interface-id</td>
<td>Specify a physical port to configure, and enter interface configuration mode. Valid interfaces include physical ports. For a PAgP EtherChannel, you can configure up to eight ports of the same type and speed for the same group. For a LACP EtherChannel, you can configure up to 16 Ethernet ports of the same type. Up to eight ports can be active, and up to eight ports can be in standby mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>switchport mode {access</td>
<td>Assign all ports as static-access ports in the same VLAN, or configure them as trunks. If you configure the port as a static-access port, assign it to only one VLAN. The range is 1 to 4094.</td>
</tr>
<tr>
<td>trunk} switchport access vlan vlan-id</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 35 Configuring EtherChannels and Link-State Tracking

Configuring EtherChannels

To remove a port from the EtherChannel group, use the **no channel-group** interface configuration command.

### Step 4

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>channel-group channel-group-number mode</code></td>
<td>Assign the port to a channel group, and specify the PAgP or the LACP mode. For <code>channel-group-number</code>, the range is 1 to 12. For <code>mode</code>, select one of these keywords:</td>
</tr>
</tbody>
</table>
| `{auto [non-silent] | desirable [non-silent] | on} | {active | passive}` | - **auto**—Enables PAgP only if a PAgP device is detected. It places the port into a passive negotiating state, in which the port responds to PAgP packets it receives but does not start PAgP packet negotiation.  
- **desirable**—Unconditionally enables PAgP. It places the port into an active negotiating state, in which the port starts negotiations with other ports by sending PAgP packets.  
- **on**—Forces the port to channel without PAgP or LACP. With the `on` mode, a usable EtherChannel exists only when a port group in the `on` mode is connected to another port group in the `on` mode.  
- **non-silent**—(Optional) If your switch is connected to a partner that is PAgP-capable, configure the switch port for nonsilent operation when the port is in the `auto` or `desirable` mode. If you do not specify `non-silent`, silent is assumed. The silent setting is for connections to file servers or packet analyzers. This setting allows PAgP to operate, to attach the port to a channel group, and to use the port for transmission.  
- **active**—Enables LACP only if a LACP device is detected. It places the port into an active negotiating state in which the port starts negotiations with other ports by sending LACP packets.  
- **passive**—Enables LACP on the port and places it into a passive negotiating state in which the port responds to LACP packets that it receives, but does not start LACP packet negotiation.  

For information on compatible modes for the switch and its partner, see the “PAgP Modes” section on page 35-4 and the “LACP Modes” section on page 35-5. |

### Step 5

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

### Step 6

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show running-config</code></td>
<td>Verify your entries.</td>
</tr>
</tbody>
</table>

### Step 7

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To remove a port from the EtherChannel group, use the **no channel-group** interface configuration command.
This example shows how to configure an EtherChannel. It assigns two ports as static-access ports in VLAN 10 to channel 5 with the PAgP mode desirable:

```sh
cSwitch# configure terminal
cSwitch(config)# interface range fastethernet1/0/4 -5
cSwitch(config-if-range)# switchport mode access
cSwitch(config-if-range)# switchport access vlan 10
cSwitch(config-if-range)# channel-group 5 mode desirable non-silent
cSwitch(config-if-range)# end
```

This example shows how to configure an EtherChannel. It assigns two ports as static-access ports in VLAN 10 to channel 5 with the LACP mode active:

```sh
cSwitch# configure terminal
cSwitch(config)# interface range gigabitethernet1/0/1 -2
cSwitch(config-if-range)# switchport mode access
cSwitch(config-if-range)# switchport access vlan 10
cSwitch(config-if-range)# channel-group 5 mode active
cSwitch(config-if-range)# end
```

### Configuring Layer 3 EtherChannels

To configure Layer 3 EtherChannels, you create the port-channel logical interface and then put the Ethernet ports into the port-channel as described in the next two sections.

### Creating Port-Channel Logical Interfaces

When configuring Layer 3 EtherChannels, you should first manually create the port-channel logical interface by using the `interface port-channel` global configuration command. Then you put the logical interface into the channel group by using the `channel-group` interface configuration command.

**Note**

To move an IP address from a physical port to an EtherChannel, you must delete the IP address from the physical port before configuring it on the port-channel interface. Beginning in privileged EXEC mode, follow these steps to create a port-channel interface for a Layer 3 EtherChannel. This procedure is required.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>interface port-channel <em>port-channel-number</em></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>no switchport</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>ip address <em>ip-address mask</em></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>show etherchannel <em>channel-group-number</em> detail</td>
</tr>
</tbody>
</table>
Chapter 35 Configuring EtherChannels and Link-State Tracking

Configuring EtherChannels

To remove the port-channel, use the `no interface port-channel port-channel-number` global configuration command.

This example shows how to create logical port-channel 5 and assign 172.10.20.10 as its IP address:

```
Switch# configure terminal
Switch(config)# interface port-channel 5
Switch(config-if)# no switchport
Switch(config-if)# ip address 172.10.20.10 255.255.255.0
Switch(config-if)# end
```

Configuring the Physical Interfaces

Beginning in privileged EXEC mode, follow these steps to assign an Ethernet port to a Layer 3 EtherChannel. This procedure is required.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> interface interface-id</td>
<td>Specify a physical port to configure, and enter interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong> no ip address</td>
<td>Ensure that there is no IP address assigned to the physical port.</td>
</tr>
<tr>
<td><strong>Step 4</strong> no switchport</td>
<td>Put the port into Layer 3 mode.</td>
</tr>
</tbody>
</table>
**Configuring EtherChannels**

**Step 5**

```
channel-group channel-group-number mode
{ auto [ non-silent ] | desirable [ non-silent ] | on } | { active | passive }
```

Assign the port to a channel group, and specify the PAgP or the LACP mode.

For `channel-group-number`, the range is 1 to 12. This number must be the same as the `port-channel-number` (logical port) configured in the “Creating Port-Channel Logical Interfaces” section on page 35-13.

For `mode`, select one of these keywords:

- **auto**—Enables PAgP only if a PAgP device is detected. It places the port into a passive negotiating state, in which the port responds to PAgP packets it receives but does not start PAgP packet negotiation.
- **desirable**—Unconditionally enables PAgP. It places the port into an active negotiating state, in which the port starts negotiations with other ports by sending PAgP packets.
- **on**—Forces the port to channel without PAgP or LACP. With the `on` mode, a usable EtherChannel exists only when a port group in the `on` mode is connected to another port group in the `on` mode.
- **non-silent**—(Optional) If your switch is connected to a partner that is PAgP capable, configure the switch port for nonsilent operation when the port is in the `auto` or `desirable` mode. If you do not specify `non-silent`, silent is assumed. The silent setting is for connections to file servers or packet analyzers. This setting allows PAgP to operate, to attach the port to a channel group, and to use the port for transmission.
- **active**—Enables LACP only if a LACP device is detected. It places the port into an active negotiating state in which the port starts negotiations with other ports by sending LACP packets.
- **passive**—Enables LACP on the port and places it into a passive negotiating state in which the port responds to LACP packets that it receives, but does not start LACP packet negotiation.

For information on compatible modes for the switch and its partner, see the “PAgP Modes” section on page 35-4 and the “LACP Modes” section on page 35-5.

**Step 6**

```
end
```

Return to privileged EXEC mode.

**Step 7**

```
show running-config
```

Verify your entries.

**Step 8**

```
copy running-config startup-config
```

(Optional) Save your entries in the configuration file.
This example shows how to configure an EtherChannel. It assigns two ports to channel 5 with the LACP mode active:

```
Switch# configure terminal
Switch(config)# interface range fastethernet1/0/4 -5
Switch(config-if-range)# no ip address
Switch(config-if-range)# no switchport
Switch(config-if-range)# channel-group 5 mode active
Switch(config-if-range)# end
```

### Configuring EtherChannel Load Balancing

This section describes how to configure EtherChannel load balancing by using source-based or destination-based forwarding methods. For more information, see the “Load Balancing and Forwarding Methods” section on page 35-6.

Beginning in privileged EXEC mode, follow these steps to configure EtherChannel load balancing. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
</tbody>
</table>
| Step 2 port-channel load-balance {dst-ip | dst-mac | src-dst-ip | src-dst-mac | src-ip | src-mac} | Configure an EtherChannel load-balancing method. The default is src-mac.

Select one of these load-distribution methods:

- **dst-ip**—Load distribution is based on the destination-host IP address.
- **dst-mac**—Load distribution is based on the destination-host MAC address of the incoming packet.
- **src-dst-ip**—Load distribution is based on the source-and-destination host-IP address.
- **src-dst-mac**—Load distribution is based on the source-and-destination host-MAC address.
- **src-ip**—Load distribution is based on the source-host IP address.
- **src-mac**—Load distribution is based on the source-MAC address of the incoming packet.

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

To return EtherChannel load balancing to the default configuration, use the `no port-channel load-balance` global configuration command.
Configuring the PAgP Learn Method and Priority

Network devices are classified as PAgP physical learners or aggregate-port learners. A device is a physical learner if it learns addresses by physical ports and directs transmissions based on that knowledge. A device is an aggregate-port learner if it learns addresses by aggregate (logical) ports. The learn method must be configured the same at both ends of the link.

When a device and its partner are both aggregate-port learners, they learn the address on the logical port-channel. The device sends packets to the source by using any of the ports in the EtherChannel. With aggregate-port learning, it is not important on which physical port the packet arrives.

PAgP cannot automatically detect when the partner device is a physical learner and when the local device is an aggregate-port learner. Therefore, you must manually set the learning method on the local device to learn addresses by physical ports. You also must set the load-distribution method to source-based distribution, so that any given source MAC address is always sent on the same physical port.

You also can configure a single port within the group for all transmissions and use other ports for hot standby. The unused ports in the group can be swapped into operation in just a few seconds if the selected single port loses hardware-signal detection. You can configure which port is always selected for packet transmission by changing its priority with the `pagp port-priority` interface configuration command. The higher the priority, the more likely that the port will be selected.

The switch supports address learning only on aggregate ports even though the `physical-port` keyword is provided in the CLI. The `pagp learn-method` command and the `pagp port-priority` command have no effect on the switch hardware, but they are required for PAgP interoperability with devices that only support address learning by physical ports, such as the Catalyst 1900 switch.

When the link partner to the switch is a physical learner (such as a Catalyst 1900 series switch), we recommend that you configure the switch as a physical-port learner by using the `pagp learn-method physical-port` interface configuration command. Set the load-distribution method based on the source MAC address by using the `port-channel load-balance src-mac` global configuration command. The switch then sends packets to the Catalyst 1900 switch using the same port in the EtherChannel from which it learned the source address. Use the `pagp learn-method` command only in this situation.

Beginning in privileged EXEC mode, follow these steps to configure your switch as a PAgP physical-port learner and to adjust the priority so that the same port in the bundle is selected for sending packets. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><code>interface interface-id</code></td>
<td>Specify the port for transmission, and enter interface configuration mode.</td>
</tr>
</tbody>
</table>
### Configuring EtherChannels

**Step 3**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>pagp learn-method physical-port</td>
<td>Select the PAgP learning method. By default, <strong>aggregation-port learning</strong> is selected, which means the switch sends packets to the source by using any of the ports in the EtherChannel. With aggregate-port learning, it is not important on which physical port the packet arrives. Select <strong>physical-port</strong> to connect with another switch that is a physical learner. Make sure to configure the <strong>port-channel load-balance</strong> global configuration command to <strong>src-mac</strong> as described in the “Configuring EtherChannel Load Balancing” section on page 35-16. The learning method must be configured the same at both ends of the link.</td>
</tr>
</tbody>
</table>

**Step 4**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>pagp port-priority priority</td>
<td>Assign a priority so that the selected port is chosen for packet transmission. For <strong>priority</strong>, the range is 0 to 255. The default is 128. The higher the priority, the more likely that the port will be used for PAgP transmission.</td>
</tr>
</tbody>
</table>

**Step 5**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

**Step 6**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td>show pagp channel-group-number internal</td>
<td></td>
</tr>
</tbody>
</table>

**Step 7**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return the priority to its default setting, use the **no pagp port-priority** interface configuration command. To return the learning method to its default setting, use the **no pagp learn-method** interface configuration command.

### Configuring LACP Hot-Standby Ports

When enabled, LACP tries to configure the maximum number of LACP-compatible ports in a channel, up to a maximum of 16 ports. Only eight LACP links can be active at one time. The software places any additional links in a hot-standby mode. If one of the active links becomes inactive, a link that is in the hot-standby mode becomes active in its place.

If you configure more than eight links for an EtherChannel group, the software automatically decides which of the hot-standby ports to make active based on the LACP priority. The software assigns to every link between systems that operate LACP a unique priority made up of these elements (in priority order):

- LACP system priority
- System ID (a combination of the LACP system priority and the switch MAC address)
- LACP port priority
- Port number

In priority comparisons, numerically lower values have higher priority. The priority decides which ports should be put in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.
Ports are considered for active use in aggregation in link-priority order starting with the port attached to the highest priority link. Each port is selected for active use if the preceding higher priority selections can also be maintained. Otherwise, the port is selected for standby mode.

You can change the default values of the LACP system priority and the LACP port priority to affect how the software selects active and standby links. For more information, see the “Configuring the LACP System Priority” section on page 35-19 and the “Configuring the LACP Port Priority” section on page 35-19.

### Configuring the LACP System Priority

You can configure the system priority for all of the EtherChannels that are enabled for LACP by using the `lacp system-priority` global configuration command. You cannot configure a system priority for each LACP-configured channel. By changing this value from the default, you can affect how the software selects active and standby links.

You can use the `show etherchannel summary` privileged EXEC command to see which ports are in the hot-standby mode (denoted with an `H` port-state flag).

Beginning in privileged EXEC mode, follow these steps to configure the LACP system priority. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code> Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>lacp system-priority priority</code> Configure the LACP system priority. For <code>priority</code>, the range is 1 to 65535. The default is 32768. The lower the value, the higher the system priority.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>end</code> Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>show running-config</code> or <code>show lacp sys-id</code> Verify your entries.</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>copy running-config startup-config</code> (Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return the LACP system priority to the default value, use the `no lacp system-priority` global configuration command.

### Configuring the LACP Port Priority

By default, all ports use the same port priority. If the local system has a lower value for the system priority and the system ID than the remote system, you can affect which of the hot-standby links become active first by changing the port priority of LACP EtherChannel ports to a lower value than the default. The hot-standby ports that have lower port numbers become active in the channel first. You can use the `show etherchannel summary` privileged EXEC command to see which ports are in the hot-standby mode (denoted with an `H` port-state flag).

**Note** If LACP is not able to aggregate all the ports that are compatible (for example, the remote system might have more restrictive hardware limitations), all the ports that cannot be actively included in the EtherChannel are put in the hot-standby state and are used only if one of the channeled ports fails.
Beginning in privileged EXEC mode, follow these steps to configure the LACP port priority. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>lACP port-priority priority</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>show running-config</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To return the LACP port priority to the default value, use the `no lACP port-priority` interface configuration command.

### Displaying EtherChannel, PAgP, and LACP Status

To display EtherChannel, PAgP, and LACP status information, use the privileged EXEC commands described in Table 35-4:

**Table 35-4 Commands for Displaying EtherChannel, PAgP, and LACP Status**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show etherchannel [channel-group-number] {detail</td>
<td>port</td>
</tr>
<tr>
<td>show pagp [channel-group-number] {counters</td>
<td>internal</td>
</tr>
<tr>
<td>show lacp [channel-group-number] {counters</td>
<td>internal</td>
</tr>
</tbody>
</table>

You can clear PAgP channel-group information and traffic counters by using the `clear pagp` {channel-group-number counters | counters} privileged EXEC command.

You can clear LACP channel-group information and traffic counters by using the `clear lacp` {channel-group-number counters | counters} privileged EXEC command.

For detailed information about the fields in the displays, see the command reference for this release.
Understanding Link-State Tracking

Link-state tracking, also known as trunk failover, is a feature that binds the link state of multiple interfaces. For example, link-state tracking provides redundancy in the network when used with Flex Links. If the link is lost on the primary interface, connectivity is transparently switched to the secondary interface.

As shown in Figure 35-4, Catalyst 3750 Metro switches are used as user-facing provider edge (UPE) switches in a customer site at the edge of the provider network connected to a customer premises equipment (CPE) switch. The UPE switches are connected to the provider edge (PE) switches in the service provider (SP) network. Customer devices, such as clients, connected to the CPE switch have multiple connections to the SP network. This configuration ensures that the traffic flow is balanced from the customer site to the SP and the reverse. Ports connected to the CPE are referred to as downstream ports, and ports connected to PE switches are referred to as upstream ports.

- UPE switch A provides links to the CPE through link-state group 1. Port 1 and port 2 are connected to the CPE. Port 3 and port 4 are connected to PE switch A through link-state group 1.
- UPE switch B provides links to the CPE through link-state group 2. Port 1 and port 2 are connected to CPE. Port 3 and 4 are connected to PE switch A through link-state group 2.

When you enable link-state tracking on the switch, the link states of the downstream ports is bound to the link states of one or more of the upstream ports. After you associate a set of downstream ports to a set of upstream ports, if all of the upstream ports become unavailable, link-state tracking automatically puts the associated downstream ports in an error-disabled state. This causes the CPE primary interface to failover to the secondary interface.

If the PE switch fails, the cables are disconnected, or the link is lost, the upstream interfaces can lose connectivity. When link-state tracking is not enabled and the upstream interfaces lose connectivity, the link states of the downstream interfaces remain unchanged. The CPE is not aware that upstream connectivity has been lost and does not failover to the secondary interface.

An interface can be an aggregation of ports (an EtherChannel), a single physical port in access or trunk mode. These interfaces can be bundled together, and each downstream interface can be associated with a single group consisting of multiple upstream interfaces, referred to as a link-state group.

In a link-state group, the link states of the downstream interfaces are dependent on the link states of the upstream interfaces. If all of the upstream interfaces in a link-state group are in the link-down state, the associated downstream interfaces are forced into the link-down state. If any one of the upstream interfaces in the link-state group in the link-up state, the associated downstream interfaces can change to or remain in a link-up state.

For example, in Figure 35-4, downstream interfaces 1 and 2 on UPE switch A are defined in link-state group 1 with upstream interfaces 3 and 4. Similarly, downstream interfaces 1 and 2 on UPE switch B are defined in link-state group 2 with upstream interfaces 3 and 4.

If the link is lost on upstream interface 3, the link states of downstream interfaces 1 and 2 do not change. If upstream interface 4 also loses link, downstream interfaces 1 and 2 change to the link-down state. The CPE switch stops forwarding traffic to PE switch A and starts to forward traffic to PE switch B.

You can recover a downstream interface link-down condition by removing the failed downstream port from the link-state group. To recover multiple downstream interfaces, disable the link-state group.
Configuring Link-State Tracking

These sections describe how to configure link-state tracking ports:
- Default Link-State Tracking Configuration, page 35-22
- Link-State Tracking Configuration Guidelines, page 35-22
- Configuring Link-State Tracking, page 35-23

Default Link-State Tracking Configuration

There are no link-state groups defined, and link-state tracking is not enabled for any group.

Link-State Tracking Configuration Guidelines

Follow these guidelines to avoid configuration problems:
- An interface that is defined as an upstream interface cannot also be defined as a downstream interface in the same or a different link-state group. The reverse is also true.
- An interface cannot be a member of more than one link-state group.
- Do not configure an EtherChannel as a downstream interface.
Configuring Link-State Tracking

Beginning in privileged EXEC mode, follow these steps to configure a link-state group and to assign an interface to a group:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>link state track number</td>
</tr>
<tr>
<td>Step 3</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 4</td>
<td>link state group [number] [upstream</td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
</tr>
<tr>
<td>Step 6</td>
<td>show running-config</td>
</tr>
<tr>
<td>Step 7</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

This example shows how to create a link-state group and configure the interfaces:

```
Switch# configure terminal
Switch(config)# link state track 1
Switch(config)# interface range fastethernet1/0/9 -10
Switch(config-if)# link state group 1 upstream
Switch(config-if)# interface fastethernet1/0/1
Switch(config-if)# link state group 1 downstream
Switch(config-if)# interface fastethernet1/0/3
Switch(config-if)# link state group 1 downstream
Switch(config-if)# interface fastethernet1/0/5
Switch(config-if)# link state group 1 downstream
Switch(config-if)# end
```

To disable a link-state group, use the no link state track number global configuration command.

Displaying Link-State Tracking Status

Use the show link state group command to display the link-state group information. Enter this command without keywords to display information about all link-state groups. Enter the group number to display information specific to the group. Enter the detail keyword to display detailed information about the group.

This is an example of output from the show link state group 1 command:

```
Switch> show link state group 1
```
Link State Group: 1  Status: Enabled, Down

This is an example of output from the show link state group detail command:

Switch> show link state group detail

(Up): Interface up  (Dwn): Interface Down  (Dis): Interface disabled

Link State Group: 1 Status: Enabled, Down
Upstream Interfaces: Fast/0/15(Dwn) Fast/0/16(Dwn)
Downstream Interfaces: Fast/0/11(Dis) Fast/0/12(Dis) Fast/0/13(Dis) Fast/0/14(Dis)

Link State Group: 2 Status: Enabled, Down
Upstream Interfaces: Fast/0/15(Dwn) Fast/0/16(Dwn) Fast/0/17(Dwn)
Downstream Interfaces: Fast/0/11(Dis) Fast/0/12(Dis) Fast/0/13(Dis) Fast/0/14(Dis)

(Up): Interface up  (Dwn): Interface Down  (Dis): Interface disabled

For detailed information about the fields in the display, see the command reference for this release.
CHAPTER 36

Configuring IP Unicast Routing

This chapter describes how to configure IP unicast routing on the Catalyst 3750 Metro switch. For more detailed IP unicast configuration information, see the *Cisco IOS IP Configuration Guide, Release 12.2*. For complete syntax and usage information for the commands used in this chapter, see these command references:

- *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2*
- *Cisco IOS IP Command Reference, Volume 3 of 3: Multicast, Release 12.2*

This chapter consists of these sections:

- Understanding IP Routing, page 36-2
- Steps for Configuring Routing, page 36-2
- Configuring IP Addressing, page 36-3
- Enabling IP Unicast Routing, page 36-17
- Configuring RIP, page 36-18
- Configuring OSPF, page 36-23
- Configuring EIGRP, page 36-35
- Configuring BGP, page 36-43
- Configuring ISO CLNS Routing, page 36-64
- Configuring BFD, page 36-73
- Configuring Multi-VRF CE, page 36-83
- Configuring Protocol-Independent Features, page 36-98
- Monitoring and Maintaining the IP Network, page 36-112

**Note**

When configuring routing parameters on the switch and to allocate system resources to maximize the number of unicast routes allowed, you can use the `sdm prefer routing` global configuration command to set the Switch Database Management (SDM) feature to the routing template. For more information on the SDM templates, see Chapter 6, “Configuring SDM Templates,” or see the `sdm prefer` command in the command reference for this release.
Understanding IP Routing

In some network environments, VLANs are associated with individual networks or subnetworks. In an IP network, each subnetwork is mapped to an individual VLAN. Configuring VLANs helps control the size of the broadcast domain and keeps local traffic local. However, network devices in different VLANs cannot communicate with one another without a Layer 3 device (router) to route traffic between the VLAN, referred to as inter-VLAN routing. You configure one or more routers to route traffic to the appropriate destination VLAN.

Figure 36-1 shows a basic routing topology. Switch A is in VLAN 10, and Switch B is in VLAN 20. The router has an interface in each VLAN.

![Routing Topology Example](image)

When Host A in VLAN 10 needs to communicate with Host B in VLAN 10, it sends a packet addressed to that host. Switch A forwards the packet directly to Host B, without sending it to the router.

When Host A sends a packet to Host C in VLAN 20, Switch A forwards the packet to the router, which receives the traffic on the VLAN 10 interface. The router checks the routing table, determines the correct outgoing interface, and forwards the packet on the VLAN 20 interface to Switch B. Switch B receives the packet and forwards it to Host C.

Routers and Layer 3 switches can route packets in three different ways:

- By using default routing
- By using preprogrammed static routes for the traffic
  
  Static unicast routing forwards packets from predetermined ports through a single path into and out of a network. Static routing does not automatically respond to changes in the network and therefore, might result in unreachable destinations.
- By dynamically calculating routes by using a routing protocol
  
  Dynamic routing protocols are used by routers to dynamically calculate the best route for forwarding traffic. Routing protocols supported by the switch are Routing Information Protocol (RIP), Border Gateway Protocol (BGP), Open Shortest Path First (OSPF) protocol, Enhanced IGRP (EIGRP), System-to-Intermediate System (IS-IS), and Bidirectional Forwarding Detection (BFD).

Steps for Configuring Routing

By default, IP routing is disabled on the switch, and you must enable it before routing can take place. For detailed IP routing configuration information, see the *Cisco IOS IP Configuration Guide, Release 12.2*. 
In the following procedures, the specified interface must be one of these Layer 3 interfaces:

- A routed port: a physical port configured as a Layer 3 port by using the `no switchport` interface configuration command.

- A switch virtual interface (SVI): a VLAN interface created by using the `interface vlan vlan_id` global configuration command and by default a Layer 3 interface.

- An EtherChannel port channel in Layer 3 mode: a port-channel logical interface created by using the `interface port-channel port-channel-number` global configuration command and binding the Ethernet interface into the channel group. For more information, see the “Configuring Layer 3 EtherChannels” section on page 35-13.

**Note**
The switch does not support tunnel interfaces for unicast routed traffic.

All Layer 3 interfaces on which routing will occur must have IP addresses assigned to them. See the “Assigning IP Addresses to Network Interfaces” section on page 36-4.

**Note**
A Layer 3 switch can have an IP address assigned to each routed port and SVI. The number of routed ports and SVIs that you can configure is not limited by software. However, the interrelationship between this number and the number and volume of features being implemented might have an impact on CPU utilization because of hardware limitations. To optimize system memory for routing, use the `sdm prefer routing` global configuration command.

Configuring routing consists of several main procedures:

- To support VLAN interfaces, create and configure VLANs on the switch, and assign VLAN membership to Layer 2 interfaces. For more information, see Chapter 11, “Configuring VLANs.”

- Configure Layer 3 interfaces.

- Enable IP routing on the switch.

- Assign IP addresses to the Layer 3 interfaces.

- Enable selected routing protocols on the switch.

- Configure routing protocol parameters (optional).

### Configuring IP Addressing

A required task for configuring IP routing is to assign IP addresses to Layer 3 network interfaces to enable the interfaces and allow communication with the hosts on those interfaces that use IP. These sections describe how to configure various IP addressing features. Assigning IP addresses to the interface is required; the other procedures are optional.

- Default Addressing Configuration, page 36-4
- Assigning IP Addresses to Network Interfaces, page 36-4
- Configuring Address Resolution Methods, page 36-7
- Routing Assistance When IP Routing is Disabled, page 36-10
- Configuring Broadcast Packet Handling, page 36-12
- Monitoring and Maintaining IP Addressing, page 36-16
Default Addressing Configuration

Table 36-1 shows the default addressing configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>None defined.</td>
</tr>
<tr>
<td>ARP</td>
<td>No permanent entries in the Address Resolution Protocol (ARP) cache.</td>
</tr>
<tr>
<td></td>
<td>Encapsulation: Standard Ethernet-style ARP.</td>
</tr>
<tr>
<td></td>
<td>Timeout: 14400 seconds (4 hours).</td>
</tr>
<tr>
<td>IP broadcast address</td>
<td>255.255.255.255 (all ones).</td>
</tr>
<tr>
<td>IP classless routing</td>
<td>Enabled.</td>
</tr>
<tr>
<td>IP default gateway</td>
<td>Disabled.</td>
</tr>
<tr>
<td>IP directed broadcast</td>
<td>Disabled (all IP directed broadcasts are dropped).</td>
</tr>
<tr>
<td>IP domain</td>
<td>Domain list: No domain names defined.</td>
</tr>
<tr>
<td></td>
<td>Domain lookup: Enabled.</td>
</tr>
<tr>
<td></td>
<td>Domain name: Enabled.</td>
</tr>
<tr>
<td>IP forward-protocol</td>
<td>If a helper address is defined or User Datagram Protocol (UDP) flooding is</td>
</tr>
<tr>
<td></td>
<td>configured, UDP forwarding is enabled on default ports.</td>
</tr>
<tr>
<td></td>
<td>Any-local-broadcast: Disabled.</td>
</tr>
<tr>
<td></td>
<td>Spanning Tree Protocol (STP): Disabled.</td>
</tr>
<tr>
<td></td>
<td>Turbo-flood: Disabled.</td>
</tr>
<tr>
<td>IP helper address</td>
<td>Disabled.</td>
</tr>
<tr>
<td>IP host</td>
<td>Disabled.</td>
</tr>
<tr>
<td>IRDP</td>
<td>Disabled.</td>
</tr>
<tr>
<td></td>
<td>Defaults when enabled:</td>
</tr>
<tr>
<td></td>
<td>• Broadcast IRDP advertisements.</td>
</tr>
<tr>
<td></td>
<td>• Maximum interval between advertisements: 600 seconds.</td>
</tr>
<tr>
<td></td>
<td>• Minimum interval between advertisements: 0.75 times max interval</td>
</tr>
<tr>
<td></td>
<td>• Preference: 0.</td>
</tr>
<tr>
<td>IP proxy ARP</td>
<td>Enabled.</td>
</tr>
<tr>
<td>IP routing</td>
<td>Disabled.</td>
</tr>
<tr>
<td>IP subnet-zero</td>
<td>Disabled.</td>
</tr>
</tbody>
</table>

Assigning IP Addresses to Network Interfaces

An IP address identifies a location to which IP packets can be sent. Some IP addresses are reserved for special uses and cannot be used for host, subnet, or network addresses. RFC 1166, “Internet Numbers,” contains the official description of IP addresses.
Chapter 36  Configuring IP Unicast Routing

Configuring IP Addressing

An interface can have one primary IP address. A mask identifies the bits that denote the network number in an IP address. When you use the mask to subnet a network, the mask is referred to as a subnet mask. To receive an assigned network number, contact your Internet service provider.

Beginning in privileged EXEC mode, follow these steps to assign an IP address and a network mask to a Layer 3 interface:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Enter interface configuration mode, and specify the Layer 3 interface to configure.</td>
</tr>
<tr>
<td>Step 3 no switchport</td>
<td>Remove the interface from Layer 2 configuration mode (if it is a physical interface).</td>
</tr>
<tr>
<td>Step 4 ip address ip-address subnet-mask</td>
<td>Configure the IP address and IP subnet mask.</td>
</tr>
<tr>
<td>Step 5 no shutdown</td>
<td>Enable the interface.</td>
</tr>
<tr>
<td>Step 6 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 7 show interfaces [interface-id]</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>show ip interface [interface-id]</td>
<td></td>
</tr>
<tr>
<td>show running-config interface [interface-id]</td>
<td></td>
</tr>
<tr>
<td>Step 8 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Use of Subnet Zero

Subnetting with a subnet address of zero is strongly discouraged because of the problems that can arise if a network and a subnet have the same addresses. For example, if network 131.108.0.0 is subnetted as 255.255.255.0, subnet zero would be written as 131.108.0.0, which is the same as the network address.

You can use the all ones subnet (131.108.255.0) and even though it is discouraged, you can enable the use of subnet zero if you need the entire subnet space for your IP address.

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 ip subnet-zero</td>
<td>Enable the use of subnet zero for interface addresses and routing updates.</td>
</tr>
<tr>
<td>Step 3 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4 show running-config</td>
<td>Verify your entry.</td>
</tr>
<tr>
<td>Step 5 copy running-config startup-config</td>
<td>(Optional) Save your entry in the configuration file.</td>
</tr>
</tbody>
</table>

Use the no ip subnet-zero global configuration command to restore the default and disable the use of subnet zero.
Classless Routing

By default, classless routing behavior is enabled on the switch when it is configured to route. With classless routing, if a router receives packets for a subnet of a network with no default route, the router forwards the packet to the best supernet route. A supernet consists of contiguous blocks of Class C address spaces used to simulate a single, larger address space and is designed to relieve the pressure on the rapidly depleting Class B address space.

In Figure 36-2, classless routing is enabled. When the host sends a packet to 120.20.4.1, instead of discarding the packet, the router forwards it to the best supernet route. If you disable classless routing and a router receives packets destined for a subnet of a network with no network default route, the router discards the packet.

Figure 36-2 IP Classless Routing

![IP Classless Routing Diagram](image)

In Figure 36-3, the router in network 128.20.0.0 is connected to subnets 128.20.1.0, 128.20.2.0, and 128.20.3.0. If the host sends a packet to 120.20.4.1, because there is no network default route, the router discards the packet.

Figure 36-3 No IP Classless Routing

![No IP Classless Routing Diagram](image)
To prevent the switch from forwarding packets destined for unrecognized subnets to the best supernet route possible, you can disable classless routing behavior.

Beginning in privileged EXEC mode, follow these steps to disable classless routing:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>no ip classless</td>
<td>Disable classless routing behavior.</td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>show running-config</td>
<td>Verify your entry.</td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entry in the configuration file.</td>
</tr>
</tbody>
</table>

To restore the default and have the switch forward packets destined for a subnet of a network with no network default route to the best supernet route possible, use the `ip classless` global configuration command.

## Configuring Address Resolution Methods

You can control interface-specific handling of IP by using address resolution. A device using IP can have both a local address or MAC address, which uniquely defines the device on its local segment or LAN, and a network address, which identifies the network to which the device belongs.

The local address or MAC address is known as a data link address because it is contained in the data link layer (Layer 2) section of the packet header and is read by data link (Layer 2) devices. To communicate with a device on Ethernet, the software must determine the MAC address of the device. The process of determining the MAC address from an IP address is called *address resolution*. The process of determining the IP address from the MAC address is called *reverse address resolution*.

The switch can use these forms of address resolution:

- Address Resolution Protocol (ARP) is used to associate IP address with MAC addresses. Taking an IP address as input, ARP determines the associated MAC address and then stores the IP address/MAC address association 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 or replies on IEEE 802 networks other than Ethernet is specified by the Subnetwork Access Protocol (SNAP).

- Proxy ARP helps hosts with no routing tables determine the MAC addresses of hosts on other networks or subnets. If the switch (router) receives an ARP request for a host that is not on the same interface as the ARP request sender, and if the router has all of its routes to the host through other interfaces, it generates a proxy ARP packet giving its own local data link address. The host that sent the ARP request then sends its packets to the router, which forwards them to the intended host.

Catalyst 3750 Metro switches also use the Reverse Address Resolution Protocol (RARP), which functions the same as ARP does, except that the RARP packets request an IP address instead of a local MAC address. Using RARP requires a RARP server on the same network segment as the router interface. Use the `ip rarp-server address` interface configuration command to identify the server.

For more information on RARP, see the *Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2*.

You can perform these tasks to configure address resolution:

- Define a Static ARP Cache, page 36-8
Define a Static ARP Cache

ARP and other address resolution protocols provide dynamic mapping between IP addresses and MAC addresses. Because most hosts support dynamic address resolution, you usually do not need to specify static ARP cache entries. If you must define a static ARP cache entry, you can do so globally, which installs a permanent entry in the ARP cache that the switch uses to translate IP addresses into MAC addresses. Optionally, you can also specify that the switch respond to ARP requests as if it were the owner of the specified IP address. If you do not want the ARP entry to be permanent, you can specify a timeout period for the ARP entry.

Beginning in privileged EXEC mode, follow these steps to provide static mapping between IP addresses and MAC addresses:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>arp ip-address hardware-address type</code></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>arp ip-address hardware-address type [alias]</code></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>interface interface-id</code></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>arp timeout seconds</code></td>
</tr>
<tr>
<td>Step 6</td>
<td><code>end</code></td>
</tr>
<tr>
<td>Step 7</td>
<td><code>show interfaces [interface-id]</code></td>
</tr>
<tr>
<td></td>
<td><code>show arp</code> or <code>show ip arp</code></td>
</tr>
<tr>
<td>Step 9</td>
<td><code>copy running-config startup-config</code></td>
</tr>
</tbody>
</table>

To remove an entry from the ARP cache, use the `no arp ip-address hardware-address type` global configuration command. To remove all nonstatic entries from the ARP cache, use the `clear arp-cache` privileged EXEC command.
Set ARP Encapsulation

By default, Ethernet ARP encapsulation (represented by the `arpa` keyword) is enabled on an IP interface. You can change the encapsulation methods to SNAP if required by your network.

Beginning in privileged EXEC mode, follow these steps to specify the ARP encapsulation type:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
</tbody>
</table>
| Step 3  | arp { arpa | snap } | Specify the ARP encapsulation method:  
  - arpa—Address Resolution Protocol  
  - snap—Subnetwork Address Protocol |
| Step 4  | end | Return to privileged EXEC mode. |
| Step 5  | show interfaces [interface-id] | Verify ARP encapsulation configuration on all interfaces or the specified interface. |
| Step 6  | copy running-config startup-config | (Optional) Save your entries in the configuration file. |

To disable an encapsulation type, use the `no arp arpa` or `no arp snap` interface configuration command.

Enable Proxy ARP

By default, the switch uses proxy ARP to help hosts determine MAC addresses of hosts on other networks or subnets.

Beginning in privileged EXEC mode, follow these steps to enable proxy ARP if it has been disabled:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>ip proxy-arp</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
</tr>
<tr>
<td>Step 5</td>
<td>show ip interface [interface-id]</td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To disable proxy ARP on the interface, use the `no ip proxy-arp` interface configuration command.
## Routing Assistance When IP Routing is Disabled

These mechanisms allow the switch to learn about routes to other networks when it does not have IP routing enabled:

- Proxy ARP, page 36-10
- Default Gateway, page 36-10
- ICMP Router Discovery Protocol (IRDP), page 36-11

### Proxy ARP

Proxy ARP, the most common method for learning about other routes, enables an Ethernet host with no routing information to communicate with hosts on other networks or subnets. The host assumes that all hosts are on the same local Ethernet and that they can use ARP to determine their MAC addresses. If a switch receives an ARP request for a host that is not on the same network as the sender, the switch evaluates whether it has the best route to that host. If it does, it sends an ARP reply packet with its own Ethernet MAC address, and the host that sent the request sends the packet to the switch, which forwards it to the intended host. Proxy ARP treats all networks as if they are local and performs ARP requests for every IP address.

Proxy ARP is enabled by default. To enable it after it has been disabled, see the “Enable Proxy ARP” section on page 36-9. Proxy ARP works as long as other routers support it.

### Default Gateway

Another method for locating routes is to define a default router or default gateway. All nonlocal packets are sent to this router, which either routes them appropriately or sends an IP Control Message Protocol (ICMP) redirect message back, defining which local router the host should use. The switch caches the redirect messages and forwards each packet as efficiently as possible. A limitation of this method is that there is no means of detecting when the default router has gone down or is unavailable.

Beginning in privileged EXEC mode, follow these steps to define a default gateway (router) when IP routing is disabled:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>ip default-gateway ip-address</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>show ip redirects</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

Use the **no ip default-gateway** global configuration command to disable this function.
ICMP Router Discovery Protocol (IRDP)

Router discovery allows the switch to dynamically learn about routes to other networks using IRDP. IRDP allows hosts to locate routers. When operating as a client, the switch generates router discovery packets. When operating as a host, the switch receives router discovery packets. The switch can also listen to Routing Information Protocol (RIP) updates and use this information to infer locations of routers. The switch does not actually store the routing tables sent by routing devices; it merely keeps track of which systems are sending the data. The advantage of using IRDP is that it allows each router to specify both a priority and the time after which a device is assumed to be down if no further packets are received.

Each device discovered becomes a candidate for the default router, and a new highest-priority router is selected when a higher priority router is discovered, when the current default router is declared down, or when a TCP connection is about to time out because of excessive retransmissions.

The only required task for IRDP routing on an interface is to enable IRDP processing on that interface. When enabled, the default parameters apply. You can optionally change any of these parameters.

Beginning in privileged EXEC mode, follow these steps to enable and configure IRDP on an interface:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id Enter interface configuration mode, and specify the Layer 3 interface to configure.</td>
</tr>
<tr>
<td>Step 3</td>
<td>ip irdp Enable IRDP processing on the interface.</td>
</tr>
<tr>
<td>Step 4</td>
<td>ip irdp multicast (Optional) Send IRDP advertisements to the multicast address (224.0.0.1) instead of IP broadcasts.</td>
</tr>
<tr>
<td></td>
<td>Note This command allows for compatibility with Sun Microsystems Solaris, which requires IRDP packets to be sent out as multicasts. Many implementations cannot receive these multicasts; ensure end-host ability before using this command.</td>
</tr>
<tr>
<td>Step 5</td>
<td>ip irdp holdtime seconds (Optional) Set the IRDP period for which advertisements are valid. The default is three times the maxadvertinterval value. It must be greater than maxadvertinterval and cannot be greater than 9000 seconds. If you change the maxadvertinterval value, this value also changes.</td>
</tr>
<tr>
<td>Step 6</td>
<td>ip irdp maxadvertinterval seconds (Optional) Set the IRDP maximum interval between advertisements. The default is 600 seconds.</td>
</tr>
<tr>
<td>Step 7</td>
<td>ip irdp minadvertinterval seconds (Optional) Set the IRDP minimum interval between advertisements. The default is 0.75 times the maxadvertinterval. If you change the maxadvertinterval, this value changes to the new default (0.75 of maxadvertinterval).</td>
</tr>
<tr>
<td>Step 8</td>
<td>ip irdp preference number (Optional) Set a device IRDP preference level. The allowed range is (-2^{31}) to (2^{31}). The default is 0. A higher value increases the router preference level.</td>
</tr>
<tr>
<td>Step 9</td>
<td>ip irdp address address [number] (Optional) Specify an IRDP address and preference to proxy-advertise.</td>
</tr>
<tr>
<td>Step 10</td>
<td>end Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 11</td>
<td>show ip irdp Verify settings by displaying IRDP values.</td>
</tr>
<tr>
<td>Step 12</td>
<td>copy running-config startup-config (Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
If you change the maxadvertinterval value, the holdtime and minadvertinterval values also change, so it is important to first change the maxadvertinterval value, before manually changing either the holdtime or minadvertinterval values.

Use the no ip irdp interface configuration command to disable IRDP routing.

### Configuring Broadcast Packet Handling

After configuring an IP interface address, you can enable routing and configure one or more routing protocols, or you can configure the way the switch responds to network broadcasts. A broadcast is a data packet destined for all hosts on a physical network. The switch supports two kinds of broadcasting:

- A directed broadcast packet is sent to a specific network or series of networks. A directed broadcast address includes the network or subnet fields.
- A flooded broadcast packet is sent to every network.

You can also limit broadcast, unicast, and multicast traffic on Layer 2 interfaces by using the storm-control interface configuration command to set traffic suppression levels. For more information, see Chapter 24, “Configuring Port-Based Traffic Control.”

Routers provide some protection from broadcast storms by limiting their extent to the local cable. Bridges (including intelligent bridges), because they are Layer 2 devices, forward broadcasts to all network segments, thus propagating broadcast storms. The best solution to the broadcast storm problem is to use a single broadcast address scheme on a network. In most modern IP implementations, you can set the address to be used as the broadcast address. Many implementations, including the one in the Catalyst 3750 switch, support several addressing schemes for forwarding broadcast messages.

Perform the tasks in these sections to enable these schemes:

- Enabling Directed Broadcast-to-Physical Broadcast Translation, page 36-12
- Forwarding UDP Broadcast Packets and Protocols, page 36-13
- Establishing an IP Broadcast Address, page 36-14
- Flooding IP Broadcasts, page 36-15

### Enabling Directed Broadcast-to-Physical Broadcast Translation

By default, IP directed broadcasts are dropped; they are not forwarded. Dropping IP-directed broadcasts makes routers less susceptible to denial-of-service attacks.

You can enable forwarding of IP-directed broadcasts on an interface where the broadcast becomes a physical (MAC-layer) broadcast. Only those protocols configured by using the ip forward-protocol global configuration command are forwarded.

You can specify an access list to control which broadcasts are forwarded. When an access list is specified, only those IP packets permitted by the access list are eligible to be translated from directed broadcasts to physical broadcasts. For more information on access lists, see Chapter 33, “Configuring Network Security with ACLs.”

Beginning in privileged EXEC mode, follow these steps to enable forwarding of IP-directed broadcasts on an interface:
### Configuring IP Addressing

Use the `no ip directed-broadcast` interface configuration command to disable translation of directed broadcast to physical broadcasts. Use the `no ip forward-protocol` global configuration command to remove a protocol or port.

#### Forwarding UDP Broadcast Packets and Protocols

User Datagram Protocol (UDP) is an IP host-to-host layer protocol, as is TCP. UDP provides a low-overhead, connectionless session between two end systems and does not provide for acknowledgment of received datagrams. Network hosts occasionally use UDP broadcasts to determine address, configuration, and name information. If such a host is on a network segment that does not include a server, UDP broadcasts are normally not forwarded. You can remedy this situation by configuring an interface on a router to forward certain classes of broadcasts to a helper address. You can use more than one helper address per interface.

You can specify a UDP destination port to control which UDP services are forwarded. You can specify multiple UDP protocols. You can also specify the Network Disk (ND) protocol, which is used by older diskless Sun workstations and the network security protocol SDNS.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td></td>
<td>Enter interface configuration mode, and specify the interface to configure.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>ip directed-broadcast [access-list-number]</td>
</tr>
<tr>
<td></td>
<td>Enable directed broadcast-to-physical broadcast translation on the interface. You can include an access list to control which broadcasts are forwarded. When you specify an access list, only IP packets permitted by the access list can be translated.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The <code>ip directed-broadcast</code> interface configuration command can be configured on a VPN routing/forwarding (VRF) interface and is VRF aware. Directed broadcast traffic is routed only within the VRF.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>exit</td>
</tr>
<tr>
<td></td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>ip forward-protocol {udp [port]</td>
</tr>
<tr>
<td></td>
<td>Specify which protocols and ports the router forwards when forwarding broadcast packets.</td>
</tr>
<tr>
<td></td>
<td>- <strong>udp</strong>—Forward UDP datagrams.</td>
</tr>
<tr>
<td></td>
<td>- <strong>port</strong>: (Optional) Destination port that controls which UDP services are forwarded.</td>
</tr>
<tr>
<td></td>
<td>- <strong>nd</strong>—Forward ND datagrams.</td>
</tr>
<tr>
<td></td>
<td>- <strong>sdns</strong>—Forward SDNS datagrams</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>end</td>
</tr>
<tr>
<td></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>show ip interface [interface-id]</td>
</tr>
<tr>
<td></td>
<td>or</td>
</tr>
<tr>
<td></td>
<td>show running-config</td>
</tr>
<tr>
<td></td>
<td>Verify the configuration on the interface or all interfaces.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>copy running-config startup-config</td>
</tr>
<tr>
<td></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
By default, both UDP and ND forwarding are enabled if a helper address has been defined for an interface. The description for the `ip forward-protocol` interface configuration command in the *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2* lists the ports that are forwarded by default if you do not specify any UDP ports.

If you do not specify any UDP ports when you configure the forwarding of UDP broadcasts, you are configuring the router to act as a BOOTP forwarding agent. BOOTP packets carry DHCP information.

Beginning in privileged EXEC mode, follow these steps to enable forwarding UDP broadcast packets on an interface and specify the destination address:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>ip helper-address address</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>exit</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>ip forward-protocol {udp [port]</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>show ip interface [interface-id]</td>
</tr>
<tr>
<td>or</td>
<td>show running-config</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

Use the `no ip helper-address` interface configuration command to disable the forwarding of broadcast packets to specific addresses. Use the `no ip forward-protocol` global configuration command to remove a protocol or port.

**Establishing an IP Broadcast Address**

The most popular IP broadcast address (and the default) is an address consisting of all ones (255.255.255.255). However, the switch can be configured to generate any form of IP broadcast address.

Beginning in privileged EXEC mode, follow these steps to set the IP broadcast address on an interface:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>ip broadcast-address ip-address</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>show ip interface [interface-id]</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>
To restore the default IP broadcast address, use the **no ip broadcast-address** interface configuration command.

### Flooding IP Broadcasts

You can allow IP broadcasts to be flooded throughout your internetwork in a controlled fashion by using the database created by the bridging STP. Using this feature also prevents loops. To support this capability, bridging must be configured on each interface that is to participate in the flooding. If bridging is not configured on an interface, it still can receive broadcasts. However, the interface never forwards broadcasts it receives, and the router never uses that interface to send broadcasts received on a different interface.

Packets that are forwarded to a single network address using the IP helper-address mechanism can be flooded. Only one copy of the packet is sent on each network segment.

To be considered for flooding, packets must meet these criteria. (Note that these are the same conditions used to consider packet forwarding using IP helper addresses.)

- The packet must be a MAC-level broadcast.
- The packet must be an IP-level broadcast.
- The packet must be a TFTP, DNS, Time, NetBIOS, ND, or BOOTP packet, or a UDP specified by the **ip forward-protocol udp** global configuration command.
- The time-to-live (TTL) value of the packet must be at least two.

A flooded UDP datagram is given the destination address specified with the **ip broadcast-address** interface configuration command on the output interface. The destination address can be set to any address. Thus, the destination address might change as the datagram propagates through the network. The source address is never changed. The TTL value is decremented.

When a flooded UDP datagram is sent out an interface (and the destination address possibly changed), the datagram is handed to the normal IP output routines and is, therefore, subject to access lists, if they are present on the output interface.

Beginning in privileged EXEC mode, follow these steps to use the bridging spanning-tree database to flood UDP datagrams:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 ip forward-protocol spanning-tree</td>
<td>Use the bridging spanning-tree database to flood UDP datagrams.</td>
</tr>
<tr>
<td>Step 3 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4 show running-config</td>
<td>Verify your entry.</td>
</tr>
<tr>
<td>Step 5 copy running-config startup-config</td>
<td>(Optional) Save your entry in the configuration file.</td>
</tr>
</tbody>
</table>

Use the **no ip forward-protocol spanning-tree** global configuration command to disable the flooding of IP broadcasts.

In a Catalyst 3750 Metro switch, the majority of packets are forwarded in hardware; most packets do not go through the switch CPU. For those packets that do go to the CPU, you can speed up spanning tree-based UDP flooding by a factor of about four to five times by using turbo-flooding. This feature is supported over Ethernet interfaces configured for ARP encapsulation.

Beginning in privileged EXEC mode, follow these steps to increase spanning-tree-based flooding:
To disable this feature, use the `no ip forward-protocol turbo-flood` global configuration command.

### Monitoring and Maintaining IP Addressing

When the contents of a particular cache, table, or database have become or are suspected to be invalid, you can remove all its contents by using the `clear` privileged EXEC commands. Table 36-2 lists the commands for clearing contents.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>clear arp-cache</code></td>
<td>Clear the IP ARP cache and the fast-switching cache.</td>
</tr>
<tr>
<td>`clear host {name</td>
<td>*}`</td>
</tr>
<tr>
<td>`clear ip route {network [mask]</td>
<td>*}`</td>
</tr>
</tbody>
</table>

You can display specific statistics, such as the contents of IP routing tables, caches, and databases; the reachability of nodes; and the routing path that packets are taking through the network. Table 36-3 lists the privileged EXEC commands for displaying IP statistics.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show arp</code></td>
<td>Display the entries in the ARP table.</td>
</tr>
<tr>
<td><code>show hosts</code></td>
<td>Display the default domain name, style of lookup service, name server hosts, and the cached list of hostnames and addresses.</td>
</tr>
<tr>
<td><code>show ip aliases</code></td>
<td>Display IP addresses mapped to TCP ports (aliases).</td>
</tr>
<tr>
<td><code>show ip arp</code></td>
<td>Display the IP ARP cache.</td>
</tr>
<tr>
<td><code>show ip interface [interface-id]</code></td>
<td>Display the IP status of interfaces.</td>
</tr>
<tr>
<td><code>show ip irdp</code></td>
<td>Display IRDP values.</td>
</tr>
<tr>
<td><code>show ip masks address</code></td>
<td>Display the masks used for network addresses and the number of subnets using each mask.</td>
</tr>
<tr>
<td><code>show ip redirects</code></td>
<td>Display the address of a default gateway.</td>
</tr>
<tr>
<td>`show ip route [address [mask]]</td>
<td>[protocol]`</td>
</tr>
<tr>
<td><code>show ip route summary</code></td>
<td>Display the current state of the routing table in summary form.</td>
</tr>
</tbody>
</table>
Enabling IP Unicast Routing

By default, the switch is in Layer 2 switching mode and IP routing is disabled. To use the Layer 3 capabilities of the switch, you must enable IP routing.

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 ip routing</td>
<td>Enable IP routing.</td>
</tr>
<tr>
<td>Step 3 router ip_routing_protocol</td>
<td>Specify an IP routing protocol. This step might include other commands, such as specifying the networks to route with the network (RIP) router configuration command. For information on specific protocols, see sections later in this chapter and to the Cisco IOS IP Configuration Guide, Release 12.2.</td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5 show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 6 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Use the no ip routing global configuration command to disable routing.

This example shows how to enable IP routing using RIP as the routing protocol:

Switch# configure terminal
Enter configuration commands, one per line. End with Ctrl/Z.
Switch(config)# ip routing
Switch(config)# router rip
Switch(config-router)# network 10.0.0.0
Switch(config-router)# end

You can now set up parameters for the selected routing protocols as described in these sections:

- Configuring RIP, page 36-18
- Configuring OSPF, page 36-23
- Configuring EIGRP, page 36-35
- Configuring BGP, page 36-43
- Configuring ISO CLNS Routing, page 36-64
- Configuring Multi-VRF CE, page 36-83

You can also configure nonprotocol-specific features:

- Configuring Protocol-Independent Features, page 36-98
Configuring RIP

The Routing Information Protocol (RIP) is an interior gateway protocol (IGP) created for use in small, homogeneous networks. It is a distance-vector routing protocol that uses broadcast User Datagram Protocol (UDP) data packets to exchange routing information. The protocol is documented in RFC 1058. You can find detailed information about RIP in IP Routing Fundamentals, published by Cisco Press.

Using RIP, the switch sends routing information updates (advertisements) every 30 seconds. If a router does not receive an update from another router for 180 seconds or more, it marks the routes served by that router as unusable. If there is still no update after 240 seconds, the router removes all routing table entries for the non-updating router.

RIP uses hop counts to rate the value of different routes. The hop count is the number of routers that can be traversed in a route. A directly connected network has a hop count of zero; a network with a hop count of 16 is unreachable. This small range (0 to 15) makes RIP unsuitable for large networks.

If the router has a default network path, RIP advertises a route that links the router to the pseudonetwork 0.0.0.0. The 0.0.0.0 network does not exist; it is treated by RIP as a network to implement the default routing feature. The switch advertises the default network if a default was learned by RIP or if the router has a gateway of last resort and RIP is configured with a default metric. RIP sends updates to the interfaces in specified networks. If an interface’s network is not specified, it is not advertised in any RIP update.

This section briefly describes how to configure RIP. It includes this information:

- Default RIP Configuration, page 36-18
- Configuring Basic RIP Parameters, page 36-19
- Configuring RIP Authentication, page 36-21
- Configuring Summary Addresses and Split Horizon, page 36-21

Default RIP Configuration

Table 36-4 shows the default RIP configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto summary</td>
<td>Enabled.</td>
</tr>
<tr>
<td>Default-information originate</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Default metric</td>
<td>Built-in; automatic metric translations.</td>
</tr>
<tr>
<td>IP RIP authentication key-chain</td>
<td>No authentication.</td>
</tr>
<tr>
<td></td>
<td>Authentication mode: clear text.</td>
</tr>
<tr>
<td>IP RIP receive version</td>
<td>According to the <strong>version</strong> router configuration command.</td>
</tr>
<tr>
<td>IP RIP send version</td>
<td>According to the <strong>version</strong> router configuration command.</td>
</tr>
<tr>
<td>IP RIP triggered</td>
<td>According to the <strong>version</strong> router configuration command.</td>
</tr>
<tr>
<td>IP split horizon</td>
<td>Varies with media.</td>
</tr>
<tr>
<td>Neighbor</td>
<td>None defined.</td>
</tr>
<tr>
<td>Network</td>
<td>None specified.</td>
</tr>
</tbody>
</table>
Configuring RIP

To configure RIP, you enable RIP routing for a network and optionally configure other parameters. On the Catalyst 3750 Metro switch, RIP configuration commands are ignored until you configure the network number.

Beginning in privileged EXEC mode, follow these steps to enable and configure RIP:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 ip routing</td>
<td>Enable IP routing. (Required only if IP routing is disabled.)</td>
</tr>
<tr>
<td>Step 3 router rip</td>
<td>Enable a RIP routing process, and enter router configuration mode.</td>
</tr>
<tr>
<td>Step 4 network network number</td>
<td>Associate a network with a RIP routing process. You can specify multiple network commands. RIP routing updates are sent and received through interfaces only on these networks. Note You must configure a network number for RIP commands to take effect.</td>
</tr>
<tr>
<td>Step 5 neighbor ip-address</td>
<td>(Optional) Define a neighboring router with which to exchange routing information. This step allows routing updates from RIP (normally a broadcast protocol) to reach nonbroadcast networks.</td>
</tr>
<tr>
<td>Step 6 offset list [access-list number</td>
<td>name] [in</td>
</tr>
</tbody>
</table>

### Table 36-4 Default RIP Configuration (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Offset list</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Output delay</td>
<td>0 milliseconds.</td>
</tr>
<tr>
<td>Validate-update-source</td>
<td>Enabled.</td>
</tr>
<tr>
<td>Version</td>
<td>Receives RIP Version 1 and 2 packets; sends Version 1 packets.</td>
</tr>
</tbody>
</table>
### Configuring RIP

#### Step 7
**timers basic update invalid holddown flush**
((Optional) Adjust routing protocol timers. Valid ranges for all timers are 0 to 4294967295 seconds.
- **update**—The time between sending routing updates. The default is 30 seconds.
- **invalid**—The timer after which a route is declared invalid. The default is 180 seconds.
- **holddown**—The time before a route is removed from the routing table. The default is 180 seconds.
- **flush**—The amount of time for which routing updates are postponed. The default is 240 seconds.

#### Step 8
**version {1 | 2}**
((Optional) Configure the switch to receive and send only RIP Version 1 or RIP Version 2 packets. By default, the switch receives Version 1 and 2 but sends only Version 1.
You can also use the interface commands `ip rip {send | receive} version 1 | 2 | 1 2` to control what versions are used for sending and receiving on interfaces.

#### Step 9
**no auto summary**
((Optional) Disable automatic summarization. By default, the switch summarizes subprefixes when crossing classful network boundaries. Disable summarization (RIP Version 2 only) to advertise subnet and host routing information to classful network boundaries.

#### Step 10
**no validate-update-source**
(Optional) Disable validation of the source IP address of incoming RIP routing updates. By default, the switch validates the source IP address of incoming RIP routing updates and discards the update if the source address is not valid. Under normal circumstances, disabling this feature is not recommended. However, if you have a router that is off-network and you want to receive its updates, you can use this command.

#### Step 11
**output-delay delay**
(Optional) Add interpacket delay for RIP updates sent. By default, packets in a multiple-packet RIP update have no delay added between packets. If you are sending packets to a lower-speed device, you can add an interpacket delay in the range of 8 to 50 milliseconds.

#### Step 12
**end**
Return to privileged EXEC mode.

#### Step 13
**show ip protocols**
Verify your entries.

#### Step 14
**copy running-config startup-config**
((Optional) Save your entries in the configuration file.

To turn off the RIP routing process, use the **no router rip** global configuration command.
To display the parameters and current state of the active routing protocol process, use the **show ip protocols** privileged EXEC command. Use the **show ip rip database** privileged EXEC command to display summary address entries in the RIP database.
Configuring RIP Authentication

RIP Version 1 does not support authentication. If you are sending and receiving RIP Version 2 packets, you can enable RIP authentication on an interface. The key chain determines the set of keys that can be used on the interface. If a key chain is not configured, no authentication is performed, not even the default. Therefore, you must also perform the tasks in the “Managing Authentication Keys” section on page 36-111.

The switch supports two modes of authentication on interfaces for which RIP authentication is enabled: plain text and MD5. The default is plain text.

Beginning in privileged EXEC mode, follow these steps to configure RIP authentication on an interface:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>ip rip authentication key-chain name-of-chain</td>
</tr>
<tr>
<td>Step 4</td>
<td>ip rip authentication mode [text</td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
</tr>
<tr>
<td>Step 6</td>
<td>show running-config interface [interface-id]</td>
</tr>
<tr>
<td>Step 7</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To restore clear text authentication, use the no ip rip authentication mode interface configuration command. To prevent authentication, use the no ip rip authentication key-chain interface configuration command.

Configuring Summary Addresses and Split Horizon

Routers connected to broadcast-type IP networks and using distance-vector routing protocols normally use the split-horizon mechanism to reduce the possibility of routing loops. Split horizon blocks information about routes from being advertised by a router on any interface from which that information originated. This feature usually optimizes communication among multiple routers, especially when links are broken.

Note
In general, disabling split horizon is not recommended unless you are certain that your application requires it to properly advertise routes.

If you want to configure an interface running RIP to advertise a summarized local IP address pool on a network access server for dial-up clients, use the ip summary-address rip interface configuration command.

Note
If split horizon is enabled, neither autosummary nor interface IP summary addresses are advertised.

Beginning in privileged EXEC mode, follow these steps to set an interface to advertise a summarized local IP address and to disable split horizon on the interface:
Configuring RIP

To disable IP summarization, use the `no ip summary-address rip` router configuration command.

In this example, the major net is 10.0.0.0. The summary address 10.2.0.0 overrides the autosummary address of 10.0.0.0 so that 10.2.0.0 is advertised out Gigabit Ethernet port 2, and 10.0.0.0 is not advertised. In the example, if the interface is still in Layer 2 mode (the default), you must enter a `no switchport` interface configuration command before entering the `ip address` interface configuration command.

**Note**
If split horizon is enabled, neither autosummary nor interface summary addresses (those configured with the `ip summary-address rip` router configuration command) are advertised.

```plaintext
Switch(config)# router rip
Switch(config-router)# interface gigabitethernet1/0/2
Switch(config-if)# ip address 10.1.5.1 255.255.255.0
Switch(config-if)# ip summary-address rip 10.2.0.0 255.255.0.0
Switch(config-if)# no ip split-horizon
Switch(config-if)# exit
Switch(config)# router rip
Switch(config-router)# network 10.0.0.0
Switch(config-router)# neighbor 2.2.2.2 peer-group mygroup
Switch(config-router)# end
```

Configuring Split Horizon

Routers connected to broadcast-type IP networks and using distance-vector routing protocols normally use the split-horizon mechanism to reduce the possibility of routing loops. Split horizon blocks information about routes from being advertised by a router on any interface from which that information originated. This feature can optimize communication among multiple routers, especially when links are broken.

**Note**
In general, we do not recommend disabling split horizon unless you are certain that your application requires it to properly advertise routes.

Beginning in privileged EXEC mode, follow these steps to disable split horizon on the interface:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>ip address ip-address subnet-mask</td>
</tr>
<tr>
<td>Step 4</td>
<td>ip summary-address rip ip address ip-network mask</td>
</tr>
<tr>
<td>Step 5</td>
<td>no ip split horizon</td>
</tr>
<tr>
<td>Step 6</td>
<td>end</td>
</tr>
<tr>
<td>Step 7</td>
<td>show ip interface interface-id</td>
</tr>
<tr>
<td>Step 8</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>


### Configuring OSPF

This section briefly describes how to configure Open Shortest Path First (OSPF). For a complete description of the OSPF commands, see the “OSPF Commands” chapter of the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2.*

#### Note

OSPF classifies different media into broadcast, nonbroadcast multiaccess (NBMA), or point-to-point networks. Broadcast and nonbroadcast networks can also be configured as point-to-multipoint networks. Starting with Cisco IOS release 12.2(25) SEE, the switch supports all these network types.

OSPF is an Interior Gateway Protocol (IGP) designed expressly for IP networks, supporting IP subnetting and tagging of externally derived routing information. OSPF also allows packet authentication and uses IP multicast when sending and receiving packets. The Cisco Systems implementation supports RFC 1253, OSPF MIB.

The Cisco implementation conforms to the OSPF Version 2 specifications with these key features:

- Definition of stub areas is supported.
- Routes learned through any IP routing protocol can be redistributed into another IP routing protocol. At the intradomain level, this means that OSPF can import routes learned through EIGRP and RIP. OSPF routes can also be exported into RIP.
- Plain text and MD5 authentication among neighboring routers within an area is supported.
- Configurable routing interface parameters include interface output cost, retransmission interval, interface transmit delay, router priority, router dead and hello intervals, and authentication key.
- Virtual links are supported.
- Not-so-stubby-areas (NSSAs) per RFC 1587 are supported.

OSPF typically requires coordination among many internal routers, area border routers (ABRs) connected to multiple areas, and autonomous system boundary routers (ASBRs). The minimum configuration would use all default parameter values, no authentication, and interfaces assigned to areas. If you customize your environment, you must ensure coordinated configuration of all routers.

This section briefly describes how to configure OSPF. It includes this information:

- **Default OSPF Configuration**, page 36-25

---

### Command Table

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>interface interface-id</td>
<td>Enter interface configuration mode, and specify the interface to configure.</td>
</tr>
<tr>
<td>3</td>
<td>ip address ip-address subnet-mask</td>
<td>Configure the IP address and IP subnet.</td>
</tr>
<tr>
<td>4</td>
<td>no ip split-horizon</td>
<td>Disable split horizon on the interface.</td>
</tr>
<tr>
<td>5</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>6</td>
<td>show ip interface interface-id</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>7</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
- Configuring Basic OSPF Parameters, page 36-26
- Configuring OSPF Interfaces, page 36-27
- Configuring OSPF Area Parameters, page 36-30
- Configuring Other OSPF Parameters, page 36-32
- Changing LSA Group Pacing, page 36-33
- Configuring a Loopback Interface, page 36-34
- Monitoring OSPF, page 36-34
Chapter 36 Configuring IP Unicast Routing

Configuring OSPF

Default OSPF Configuration

Table 36-5 shows the default OSPF configuration.

Table 36-5  Default OSPF Configuration

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface parameters</td>
<td>Cost: No default cost predefined.</td>
</tr>
<tr>
<td></td>
<td>Retransmit interval: 5 seconds.</td>
</tr>
<tr>
<td></td>
<td>Transmit delay: 1 second.</td>
</tr>
<tr>
<td></td>
<td>Priority: 1.</td>
</tr>
<tr>
<td></td>
<td>Hello interval: 10 seconds.</td>
</tr>
<tr>
<td></td>
<td>Dead interval: 4 times the hello interval.</td>
</tr>
<tr>
<td></td>
<td>No authentication.</td>
</tr>
<tr>
<td></td>
<td>No password specified.</td>
</tr>
<tr>
<td></td>
<td>MD5 authentication disabled.</td>
</tr>
<tr>
<td>Area</td>
<td>Authentication type: 0 (no authentication).</td>
</tr>
<tr>
<td></td>
<td>Default cost: 1.</td>
</tr>
<tr>
<td></td>
<td>Range: Disabled.</td>
</tr>
<tr>
<td></td>
<td>Stub: No stub area defined.</td>
</tr>
<tr>
<td></td>
<td>NSSA: No NSSA area defined.</td>
</tr>
<tr>
<td>Auto cost</td>
<td>100 Mbps.</td>
</tr>
<tr>
<td>Default-information originate</td>
<td>Disabled. When enabled, the default metric setting is 10, and the external route type default is Type 2.</td>
</tr>
<tr>
<td>Default metric</td>
<td>Built-in, automatic metric translation, as appropriate for each routing protocol.</td>
</tr>
<tr>
<td>Distance OSPF</td>
<td>dist1 (all routes within an area): 110.</td>
</tr>
<tr>
<td></td>
<td>dist2 (all routes from one area to another): 110.</td>
</tr>
<tr>
<td></td>
<td>dist3 (routes from other routing domains): 110.</td>
</tr>
<tr>
<td>OSPF database filter</td>
<td>Disabled. All outgoing link-state advertisements (LSAs) are flooded to the interface.</td>
</tr>
<tr>
<td>IP OSPF name lookup</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Log adjacency changes</td>
<td>Enabled.</td>
</tr>
<tr>
<td>Neighbor</td>
<td>None specified.</td>
</tr>
<tr>
<td>Neighbor database filter</td>
<td>Disabled. All outgoing LSAs are flooded to the neighbor.</td>
</tr>
<tr>
<td>Network area</td>
<td>Disabled.</td>
</tr>
<tr>
<td>NSF1 awareness</td>
<td>Enabled². Allows Layer 3 switches to continue forwarding packets from a neighboring NSF-capable router during hardware or software changes.</td>
</tr>
<tr>
<td>Router ID</td>
<td>No OSPF routing process defined.</td>
</tr>
<tr>
<td>Summary address</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Timers LSA group pacing</td>
<td>240 seconds.</td>
</tr>
</tbody>
</table>
Configuring OSPF

The OSPF NSF Awareness feature is supported for IPv4, beginning with Cisco IOS Release 12.2(25)SEG. When the neighboring router is NSF-capable, the Layer 3 switch continues to forward packets from the neighboring router during the interval between the primary Route Processor (RP) in a router crashing and the backup RP taking over, or while the primary RP is manually reloaded for a non-disruptive software upgrade.

This feature cannot be disabled.

Nonstop Forwarding Awareness

The OSPF NSF Awareness feature is supported for IPv4, beginning with Cisco IOS Release 12.2(25)SEG. When the neighboring router is NSF-capable, the Layer 3 switch continues to forward packets from the neighboring router during the interval between the primary Route Processor (RP) in a router crashing and the backup RP taking over, or while the primary RP is manually reloaded for a non-disruptive software upgrade.

This feature cannot be disabled.

Configuring Basic OSPF Parameters

Enabling OSPF requires that you create an OSPF routing process, specify the range of IP addresses to be associated with the routing process, and assign area IDs to be associated with that range.

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

### Table 36-5 Default OSPF Configuration (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timers shortest path first (spf)</td>
<td>spf delay: 5 seconds. spf-holdtime: 10 seconds.</td>
</tr>
<tr>
<td>Virtual link</td>
<td>No area ID or router ID defined.</td>
</tr>
<tr>
<td></td>
<td>Hello interval: 10 seconds.</td>
</tr>
<tr>
<td></td>
<td>Retransmit interval: 5 seconds.</td>
</tr>
<tr>
<td></td>
<td>Transmit delay: 1 second.</td>
</tr>
<tr>
<td></td>
<td>Dead interval: 40 seconds.</td>
</tr>
<tr>
<td></td>
<td>Authentication key: no key predefined.</td>
</tr>
<tr>
<td></td>
<td>Message-digest key (MD5): no key predefined.</td>
</tr>
</tbody>
</table>

1. NSF = Nonstop forwarding
2. OSPF NSF awareness is enabled for IPv4 on Catalyst 3750 Metro switches, Cisco IOS Release 12.2(25)SEG or later.

### Command Purpose

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>router ospf process-id</td>
<td>Enable OSPF routing, and enter router configuration mode. The process ID is an internally used identification parameter that is locally assigned and can be any positive integer. Each OSPF routing process has a unique value.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>network address wildcard-mask area area-id</td>
<td>Define an interface on which OSPF runs and the area ID for that interface. You can use the wildcard-mask to use a single command to define one or more multiple interfaces to be associated with a specific OSPF area. The area ID can be a decimal value or an IP address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
To terminate an OSPF routing process, use the `no router ospf process-id` global configuration command.

This example shows how to configure an OSPF routing process and assign it a process number of 109:

```
Switch(config)# router ospf 109
Switch(config-router)# network 131.108.0.0 255.255.255.0 area 24
```

### Configuring OSPF Interfaces

You can use the `ip ospf` interface configuration commands to modify interface-specific OSPF parameters. You are not required to modify any of these parameters, but some interface parameters (hello interval, dead interval, and authentication key) must be consistent across all routers in an attached network. If you modify these parameters, be sure all routers in the network have compatible values.

**Note** The `ip ospf` interface configuration commands are all optional.

Beginning in privileged EXEC mode, follow these steps to modify OSPF interface parameters:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><code>interface interface-id</code></td>
<td>Enter interface configuration mode, and specify the Layer 3 interface to configure.</td>
</tr>
<tr>
<td><code>ip ospf cost</code></td>
<td>(Optional) Explicitly specify the cost of sending a packet on the interface.</td>
</tr>
<tr>
<td><code>ip ospf retransmit-interval seconds</code></td>
<td>(Optional) Specify the number of seconds between link state advertisement transmissions. The range is 1 to 65535 seconds. The default is 5 seconds.</td>
</tr>
<tr>
<td><code>ip ospf transmit-delay seconds</code></td>
<td>(Optional) Set the estimated number of seconds to wait before sending a link state update packet. The range is 1 to 65535 seconds. The default is 1 second.</td>
</tr>
<tr>
<td><code>ip ospf priority number</code></td>
<td>(Optional) Set priority to help determine the OSPF designated router for a network. The range is from 0 to 255. The default is 1.</td>
</tr>
<tr>
<td><code>ip ospf hello-interval seconds</code></td>
<td>(Optional) Set the number of seconds between hello packets sent on an OSPF interface. The value must be the same for all nodes on a network. The range is 1 to 65535 seconds. The default is 10 seconds.</td>
</tr>
<tr>
<td><code>ip ospf dead-interval seconds</code></td>
<td>(Optional) Set the number of seconds after the last device hello packet was seen before its neighbors declare the OSPF router to be down. The value must be the same for all nodes on a network. The range is 1 to 65535 seconds. The default is 4 times the hello interval.</td>
</tr>
</tbody>
</table>

To verify your entries, you can use the `show ip protocols` command.

To save your entries in the configuration file, you can use the `copy running-config startup-config` command.
Configuring OSPF

Use the no form of these commands to remove the configured parameter value or return to the default value.

### Configuring OSPF Network Types

OSPF classifies different media into the three types of networks by default:

- Broadcast networks (Ethernet, Token Ring, and FDDI)
- Nonbroadcast multiaccess (NBMA) networks (Switched Multimegabit Data Service [SMDS], Frame Relay, and X.25)
- Point-to-point networks (High-Level Data Link Control [HDLC], PPP)

You can also configure network interfaces as either a broadcast or an NBMA network and as point-to-point or point-to-multipoint, regardless of the default media type.

### Configuring OSPF for Nonbroadcast Networks

Because many routers might be attached to an OSPF network, a designated router is selected for the network. If broadcast capability is not configured in the network, the designated router selection requires special configuration parameters. You need to configure these parameters only for devices that are eligible to become the designated router or backup designated router (in other words, routers with a nonzero router priority value).
Beginning in privileged EXEC mode, follow these steps to configure routers that interconnect to nonbroadcast networks:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>router ospf process-id</td>
<td>Configure an OSPF routing process and enter router configuration mode.</td>
</tr>
</tbody>
</table>
| Step 3 | neighbor ip-address [priority number] [poll-interval seconds] | Specify an OSPF neighbor with neighbor parameters as required.  
  - ip-address—Enter the interface IP address of the OSPF neighbor.  
  - (Optional) priority number—Specify the router priority value of the nonbroadcast neighbor associated with the IP address. The range is 0 to 255; the default is 0.  
  - (Optional) poll-interval seconds—Specify a number that represents the poll interval time (in seconds). This value should be much larger than the hello interval. The range is 0-4294967295; the default is 120 seconds (2 minutes). |
| Step 4 | end               | Return to privileged EXEC mode.              |
| Step 5 | show ip ospf [process-id] | Display OSPF-related information.           |
| Step 6 | copy running-config startup-config | (Optional) Save your entries in the configuration file. |

On point-to-multipoint, nonbroadcast networks, you then use the `neighbor` router configuration command to identify neighbors. Assigning a cost to a neighbor is optional.

### Configuring Network Types for OSPF Interfaces

You can configure network interfaces as either broadcast or NBMA and as point-to point or point-to-multipoint, regardless of the default media type.

An OSPF point-to-multipoint interface is defined as a numbered point-to-point interface with one or more neighbors. On point-to-multipoint broadcast networks, specifying neighbors is optional. When you configure an interface as point-to-multipoint when the media does not support broadcast, you should use the `neighbor` command to identify neighbors.

Beginning in privileged EXEC mode, follow these steps to configure OSPF network type for an interface:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
<td>Enter interface configuration mode, and specify the Layer 3 interface to configure.</td>
</tr>
</tbody>
</table>
Use the no form of the `ip ospf network` command to return to the default network type for the media.

## Configuring OSPF Area Parameters

You can optionally configure several OSPF area parameters. These parameters include authentication for password-based protection against unauthorized access to an area, stub areas, and not-so-stubby-areas (NSSAs). **Stub areas** are areas into which information on external routes is not sent. Instead, the area border router (ABR) generates a default external route into the stub area for destinations outside the autonomous system (AS). An NSSA does not flood all LSAs from the core into the area, but can import AS external routes within the area by redistribution.
Route summarization is the consolidation of advertised addresses into a single summary route to be advertised by other areas. If network numbers are contiguous, you can use the `area range` router configuration command to configure the ABR to advertise a summary route that covers all networks in the range.

**Note**
The OSPF `area` router configuration commands are all optional.

Beginning in privileged EXEC mode, follow these steps to configure area parameters:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>router ospf process-id</td>
<td>Enable OSPF routing, and enter router configuration mode.</td>
</tr>
<tr>
<td>3</td>
<td>area area-id authentication</td>
<td>(Optional) Allow password-based protection against unauthorized access to the identified area. The identifier can be either a decimal value or an IP address.</td>
</tr>
<tr>
<td>4</td>
<td>area area-id authentication message-digest</td>
<td>(Optional) Enable MD5 authentication on the area.</td>
</tr>
<tr>
<td>5</td>
<td>area area-id stub [no-summary]</td>
<td>(Optional) Define an area as a stub area. The <code>no-summary</code> keyword prevents an ABR from sending summary link advertisements into the stub area.</td>
</tr>
</tbody>
</table>
| 6    | area area-id nssa [no-redistribution] [default-information-originate] [no-summary] | (Optional) Defines an area as a not-so-stubby-area. Every router within the same area must agree that the area is NSSA. Select one of these keywords:  
  - `no-redistribution`—Select when the router is an NSSA ABR and you want the `redistribute` command to import routes into normal areas, but not into the NSSA.  
  - `default-information-originate`—Select on an ABR to allow importing type 7 LSAs into the NSSA.  
  - `no-redistribution`—Select to not send summary LSAs into the NSSA. |
| 7    | area area-id range address mask | (Optional) Specify an address range for which a single route is advertised. Use this command only with area border routers. |
| 8    | end | Return to privileged EXEC mode. |
| 9    | show ip ospf [process-id] | Display information about the OSPF routing process in general or for a specific process ID to verify configuration. |
|      | show ip ospf [process-id [area-id]] database | Display lists of information related to the OSPF database for a specific router. |
| 10   | copy running-config startup-config | (Optional) Save your entries in the configuration file. |

Use the `no` form of these commands to remove the configured parameter value or to return to the default value.
Configuring Other OSPF Parameters

You can optionally configure other OSPF parameters in router configuration mode.

- Route summarization: When redistributing routes from other protocols as described in the “Using Route Maps to Redistribute Routing Information” section on page 36-102, each route is advertised individually in an external LSA. To help decrease the size of the OSPF link state database, you can use the **summary-address** router configuration command to advertise a single router for all the redistributed routes included in a specified network address and mask.

- Virtual links: In OSPF, all areas must be connected to a backbone area. You can establish a virtual link in case of a backbone-continuity break by configuring two Area Border Routers as endpoints of a virtual link. Configuration information includes the identity of the other virtual endpoint (the other ABR) and the nonbackbone link that the two routers have in common (the transit area). Virtual links cannot be configured through a stub area.

- Default route: When you specifically configure redistribution of routes into an OSPF routing domain, the route automatically becomes an autonomous system boundary router (ASBR). You can force the ASBR to generate a default route into the OSPF routing domain.

- Domain Name Server (DNS) names for use in all OSPF show privileged EXEC command displays makes it easier to identify a router than displaying it by router ID or neighbor ID.

- Default Metrics: OSPF calculates the OSPF metric for an interface according to the bandwidth of the interface. The metric is calculated as ref-bw divided by bandwidth, where ref is 10 by default, and bandwidth (bw) is determined by the bandwidth interface configuration command. For multiple links with high bandwidth, you can specify a larger number to differentiate the cost on those links.

- Administrative distance is a rating of the trustworthiness of a routing information source, an integer between 0 and 255, with a higher value meaning a lower trust rating. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored. OSPF uses three different administrative distances: routes within an area (interarea), routes to another area (interarea), and routes from another routing domain learned through redistribution (external). You can change any of the distance values.

- Passive interfaces: Because interfaces between two devices on an Ethernet represent only one network segment, to prevent OSPF from sending hello packets for the sending interface, you must configure the sending device to be a passive interface. Both devices can identify each other through the hello packet for the receiving interface.

- Route calculation timers: You can configure the delay time between when OSPF receives a topology change and when it starts the shortest path first (SPF) calculation and the hold time between two SPF calculations.

- Log neighbor changes: You can configure the router to send a syslog message when an OSPF neighbor state changes, providing a high-level view of changes in the router.

Beginning in privileged EXEC mode, follow these steps to configure these OSPF parameters:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>router ospf process-id</td>
<td>Enable OSPF routing, and enter router configuration mode.</td>
</tr>
<tr>
<td>3</td>
<td>summary-address address mask</td>
<td>(Optional) Specify an address and IP subnet mask for redistributed routes so that only one summary route is advertised.</td>
</tr>
</tbody>
</table>
Configuring OSPF

Changing LSA Group Pacing

The OSPF LSA group pacing feature allows the router to group OSPF LSAs and pace the refreshing, check-summing, and aging functions for more efficient router use. This feature is enabled by default with a 4-minute default pacing interval, and you will not usually need to modify this parameter. The optimum group pacing interval is inversely proportional to the number of LSAs the router is refreshing, check-summing, and aging. For example, if you have approximately 10,000 LSAs in the database, decreasing the pacing interval would benefit you. If you have a very small database (40 to 100 LSAs), increasing the pacing interval to 10 to 20 minutes might benefit you slightly.

Beginning in privileged EXEC mode, follow these steps to configure OSPF LSA pacing:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>router ospf process-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>timers lsa-group-pacing seconds</td>
</tr>
</tbody>
</table>
To return to the default value, use the **no timers lsa-group-pacing** router configuration command.

**Configuring a Loopback Interface**

OSPF uses the highest IP address configured on the interfaces as its router ID. If this interface is down or removed, the OSPF process must recalculate a new router ID and resend all its routing information out its interfaces. If a loopback interface is configured with an IP address, OSPF uses this IP address as its router ID, even if other interfaces have higher IP addresses. Because loopback interfaces never fail, this provides greater stability. OSPF automatically prefers a loopback interface over other interfaces, and it chooses the highest IP address among all loopback interfaces.

Beginning in privileged EXEC mode, follow these steps to configure a loopback interface:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>interface loopback 0</td>
<td>Create a loopback interface, and enter interface configuration mode.</td>
</tr>
<tr>
<td>ip address address mask</td>
<td>Assign an IP address to this interface.</td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>show ip interface</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Use the **no interface loopback 0** global configuration command to disable the loopback interface.

**Monitoring OSPF**

You can display specific statistics such as the contents of IP routing tables, caches, and databases.

Table 36-6 lists some of the privileged EXEC commands for displaying statistics. For more **show ip ospf database** privileged EXEC command options and for explanations of fields in the resulting display, see the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2*. 

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>interface loopback 0</td>
<td>Create a loopback interface, and enter interface configuration mode.</td>
</tr>
<tr>
<td>ip address address mask</td>
<td>Assign an IP address to this interface.</td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>show ip interface</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
Enhanced IGRP (EIGRP) is a Cisco proprietary enhanced version of the IGRP. EIGRP uses the same distance vector algorithm and distance information as IGRP; however, the convergence properties and the operating efficiency of EIGRP are significantly improved.

The convergence technology employs an algorithm referred to as the Diffusing Update Algorithm (DUAL), which guarantees loop-free operation at every instant throughout a route computation and allows all devices involved in a topology change to synchronize at the same time. Routers that are not affected by topology changes are not involved in recomputations.

IP EIGRP provides increased network width. With RIP, the largest possible width of your network is 15 hops. Because the EIGRP metric is large enough to support thousands of hops, the only barrier to expanding the network is the transport-layer hop counter. EIGRP increments the transport control field only when an IP packet has traversed 15 routers and the next hop to the destination was learned through EIGRP. When a RIP route is used as the next hop to the destination, the transport control field is incremented as usual.

EIGRP offers these features:

- Fast convergence.
- Incremental updates when the state of a destination changes, instead of sending the entire contents of the routing table, minimizing the bandwidth required for EIGRP packets.
- Less CPU usage because full update packets need not be processed each time they are received.
- Protocol-independent neighbor discovery mechanism to learn about neighboring routers.
- Variable-length subnet masks (VLSMs).
- Arbitrary route summarization.

**Table 36-6  Show IP OSPF Statistics Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip ospf [process-id] database [router] [link-state-id]</td>
<td>Display lists of information related to the OSPF database.</td>
</tr>
<tr>
<td>show ip ospf [process-id] database [router] [self-originate]</td>
<td></td>
</tr>
<tr>
<td>show ip ospf [process-id] database [router] [adv-router [ip-address]]</td>
<td></td>
</tr>
<tr>
<td>show ip ospf [process-id] database [network] [link-state-id]</td>
<td></td>
</tr>
<tr>
<td>show ip ospf [process-id] database [summary] [link-state-id]</td>
<td></td>
</tr>
<tr>
<td>show ip ospf [process-id] database [asbr-summary] [link-state-id]</td>
<td></td>
</tr>
<tr>
<td>show ip ospf [process-id] database [external] [link-state-id]</td>
<td></td>
</tr>
<tr>
<td>show ip ospf [process-id area-id] database [database-summary]</td>
<td>Display the internal OSPF routing ABR and ASBR table entries.</td>
</tr>
<tr>
<td>show ip ospf border-routes</td>
<td></td>
</tr>
<tr>
<td>show ip ospf interface [interface-name]</td>
<td>Display OSPF-related interface information.</td>
</tr>
<tr>
<td>show ip ospf neighbor [interface-name] [neighbor-id] detail</td>
<td>Display OSPF interface neighbor information.</td>
</tr>
<tr>
<td>show ip ospf virtual-links</td>
<td>Display OSPF-related virtual links information.</td>
</tr>
</tbody>
</table>

**Configuring EIGRP**
EIGRP scales to large networks.

Enhanced IGRP has these four basic components:

- **Neighbor discovery and recovery** is the process that routers use to dynamically learn of other routers on their directly attached networks. Routers must also discover when their neighbors become unreachable or inoperative. Neighbor discovery and recovery is achieved with low overhead by periodically sending small hello packets. As long as hello packets are received, the Cisco IOS software can determine that a neighbor is alive and functioning. When this status is determined, the neighboring routers can exchange routing information.

- **The reliable transport protocol** is responsible for guaranteed, ordered delivery of EIGRP packets to all neighbors. It supports intermixed transmission of multicast and unicast packets. Some EIGRP packets must be sent reliably, and others need not be. For efficiency, reliability is provided only when necessary. For example, on a multiaccess network that has multicast capabilities (such as Ethernet), it is not necessary to send hellos reliably to all neighbors individually. Therefore, EIGRP sends a single multicast hello with an indication in the packet informing the receivers that the packet need not be acknowledged. Other types of packets (such as updates) require acknowledgment, which is shown in the packet. The reliable transport has a provision to send multicast packets quickly when there are unacknowledged packets pending. Doing so helps ensure that convergence time remains low in the presence of varying speed links.

- **The DUAL finite state machine** embodies the decision process for all route computations. It tracks all routes advertised by all neighbors. DUAL uses the distance information (known as a metric) to select efficient, loop-free paths. DUAL selects routes to be inserted into a routing table based on feasible successors. A successor is a neighboring router used for packet forwarding that has a least-cost path to a destination that is guaranteed not to be part of a routing loop. When there are no feasible successors, but there are neighbors advertising the destination, a recomputation must occur. This is the process whereby a new successor is determined. The amount of time it takes to recompute the route affects the convergence time. Recomputation is processor-intensive; it is advantageous to avoid recomputation if it is not necessary. When a topology change occurs, DUAL tests for feasible successors. If there are feasible successors, it uses any it finds to avoid unnecessary recomputation.

- **The protocol-dependent modules** are responsible for network layer protocol-specific tasks. An example is the IP EIGRP module, which is responsible for sending and receiving EIGRP packets that are encapsulated in IP. It is also responsible for parsing EIGRP packets and informing DUAL of the new information received. EIGRP asks DUAL to make routing decisions, but the results are stored in the IP routing table. EIGRP is also responsible for redistributing routes learned by other IP routing protocols.

This section briefly describes how to configure EIGRP. It includes this information:

- Default EIGRP Configuration, page 36-37
- Configuring Basic EIGRP Parameters, page 36-38
- Configuring EIGRP Interfaces, page 36-39
- Configuring EIGRP Route Authentication, page 36-40
- Configuring EIGRP Stub Routing, page 36-41
- Monitoring and Maintaining EIGRP, page 36-42
## Default EIGRP Configuration

Table 36-7 shows the default EIGRP configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto summary</td>
<td>Enabled. Subprefixes are summarized to the classful network boundary when crossing classful network boundaries.</td>
</tr>
<tr>
<td>Default-information</td>
<td>Exterior routes are accepted and default information is passed between EIGRP processes when doing redistribution.</td>
</tr>
<tr>
<td>Default metric</td>
<td>Only connected routes and interface static routes can be redistributed without a default metric. The metric includes:</td>
</tr>
<tr>
<td></td>
<td>• Bandwidth: 0 or greater kbps.</td>
</tr>
<tr>
<td></td>
<td>• Delay (tens of microseconds): 0 or any positive number that is a multiple of 39.1 nanoseconds.</td>
</tr>
<tr>
<td></td>
<td>• Reliability: any number between 0 and 255 (255 means 100 percent reliability).</td>
</tr>
<tr>
<td></td>
<td>• Loading: effective bandwidth as a number between 0 and 255 (255 is 100 percent loading).</td>
</tr>
<tr>
<td></td>
<td>• MTU: maximum transmission unit size of the route in bytes. 0 or any positive integer.</td>
</tr>
<tr>
<td>Distance</td>
<td>Internal distance: 90.</td>
</tr>
<tr>
<td></td>
<td>External distance: 170.</td>
</tr>
<tr>
<td>EIGRP log-neighbor changes</td>
<td>Disabled. No adjacency changes logged.</td>
</tr>
<tr>
<td>IP authentication key-chain</td>
<td>No authentication provided.</td>
</tr>
<tr>
<td>IP authentication mode</td>
<td>No authentication provided.</td>
</tr>
<tr>
<td>IP bandwidth-percent</td>
<td>50 percent.</td>
</tr>
<tr>
<td>IP hello interval</td>
<td>For low-speed nonbroadcast multiaccess (NBMA) networks: 60 seconds; all other networks: 5 seconds.</td>
</tr>
<tr>
<td>IP hold-time</td>
<td>For low-speed NBMA networks: 180 seconds; all other networks: 15 seconds.</td>
</tr>
<tr>
<td>IP split-horizon</td>
<td>Enabled.</td>
</tr>
<tr>
<td>IP summary address</td>
<td>No summary aggregate addresses are predefined.</td>
</tr>
<tr>
<td>Metric weights</td>
<td>tos: 0; k1 and k3: 1; k2, k4, and k5: 0</td>
</tr>
<tr>
<td>Network</td>
<td>None specified.</td>
</tr>
<tr>
<td>NSF1 Awareness</td>
<td>Enabled. Allows Layer 3 switches to continue forwarding packets from a neighboring NSF-capable router during hardware or software changes.</td>
</tr>
<tr>
<td>Offset-list</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Router EIGRP</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Set metric</td>
<td>No metric set in the route map.</td>
</tr>
<tr>
<td>Traffic-share</td>
<td>Distributed proportionately to the ratios of the metrics.</td>
</tr>
<tr>
<td>Variance</td>
<td>1 (equal-cost load balancing).</td>
</tr>
</tbody>
</table>

1. NSF = Nonstop Forwarding
2. EIGRP NSF awareness is enabled for IPv4 on Catalyst 3750 Metro switches, Cisco IOS Release 12.2(25)SEG or later.
To create an EIGRP routing process, you must enable EIGRP and associate networks. EIGRP sends updates to the interfaces in the specified networks. If you do not specify an interface network, it is not advertised in any EIGRP update.

**Note**

If you have routers on your network that are configured for IGRP, and you want to change to EIGRP, you must designate transition routers that have both IGRP and EIGRP configured. In these cases, perform Steps 1 through 3 in the next section and also see the “Configuring Split Horizon” section on page 36-22. You must use the same AS number for routes to be automatically redistributed.

### Nonstop Forwarding Awareness

The EIGRP NSF Awareness feature is supported for IPv4, beginning with Cisco IOS Release 12.2(25)SEG. When the neighboring router is NSF-capable, the Layer 3 switch continues to forward packets from the neighboring router during the interval between the primary Route Processor (RP) in a router failing and the backup RP taking over, or while the primary RP is manually reloaded for a nondisruptive software upgrade.

This feature cannot be disabled. For more information on this feature, see the EIGRP Nonstop Forwarding (NSF) Awareness Feature Guide at this URL: http://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/ft_ensf.html

### Configuring Basic EIGRP Parameters

Beginning in privileged EXEC mode, follow these steps to configure EIGRP. Configuring the routing process is required; other steps are optional:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>router eigrp autonomous-system Enable an EIGRP routing process, and enter router configuration mode. The AS number identifies the routes to other EIGRP routers and is used to tag routing information.</td>
</tr>
<tr>
<td>Step 3</td>
<td>network network-number Associate networks with an EIGRP routing process. EIGRP sends updates to the interfaces in the specified networks.</td>
</tr>
<tr>
<td>Step 4</td>
<td>eigrp log-neighbor-changes (Optional) Enable logging of EIGRP neighbor changes to monitor routing system stability.</td>
</tr>
<tr>
<td>Step 5</td>
<td>metric weights  tos k1 k2 k3 k4 k5 (Optional) Adjust the EIGRP metric. Although the defaults have been carefully determined to provide excellent operation in most networks, you can adjust them.</td>
</tr>
<tr>
<td></td>
<td><strong>Caution</strong> Determining metrics is complex and is not recommended without guidance from an experienced network designer.</td>
</tr>
<tr>
<td>Step 6</td>
<td>offset list [access-list number | name] {in | out} offset [type number] (Optional) Apply an offset list to routing metrics to increase incoming and outgoing metrics to routes learned through EIGRP. You can limit the offset list with an access list or an interface.</td>
</tr>
</tbody>
</table>
### Configuring EIGRP Interfaces

Other optional EIGRP parameters can be configured on an interface basis.

Beginning in privileged EXEC mode, follow these steps to configure EIGRP interfaces:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>ip bandwidth-percent eigrp percent</td>
</tr>
<tr>
<td>Step 4</td>
<td>ip summary-address eigrp autonomous-system-number address mask</td>
</tr>
<tr>
<td>Step 5</td>
<td>ip hello-interval eigrp autonomous-system-number seconds</td>
</tr>
<tr>
<td>Step 6</td>
<td>ip hold-time eigrp autonomous-system-number seconds</td>
</tr>
<tr>
<td></td>
<td>Caution</td>
</tr>
<tr>
<td>Step 7</td>
<td>no ip split-horizon eigrp autonomous-system-number</td>
</tr>
<tr>
<td>Step 8</td>
<td>end</td>
</tr>
<tr>
<td>Step 9</td>
<td>show ip eigrp interface</td>
</tr>
<tr>
<td>Step 10</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

Use the no forms of these commands to disable the feature or return the setting to the default value.
Use the no forms of these commands to disable the feature or return the setting to the default value.

## Configuring EIGRP Route Authentication

EIGRP route authentication provides MD5 authentication of routing updates from the EIGRP routing protocol to prevent the introduction of unauthorized or false routing messages from unapproved sources.

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> interface interface-id</td>
<td>Enter interface configuration mode, and specify the Layer 3 interface to configure.</td>
</tr>
<tr>
<td><strong>Step 3</strong> ip authentication mode eigrp autonomous-system md5</td>
<td>Enable MD5 authentication in IP EIGRP packets.</td>
</tr>
<tr>
<td><strong>Step 4</strong> ip authentication key-chain eigrp autonomous-system key-chain</td>
<td>Enable authentication of IP EIGRP packets.</td>
</tr>
<tr>
<td><strong>Step 5</strong> exit</td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 6</strong> key chain name-of-chain</td>
<td>Identify a key chain and enter key-chain configuration mode. Match the name configured in Step 4.</td>
</tr>
<tr>
<td><strong>Step 7</strong> key number</td>
<td>In key-chain configuration mode, identify the key number.</td>
</tr>
<tr>
<td><strong>Step 8</strong> key-string text</td>
<td>In key-chain key configuration mode, identify the key string.</td>
</tr>
<tr>
<td><strong>Step 9</strong> accept-lifetime start-time {infinite</td>
<td>end-time</td>
</tr>
<tr>
<td><strong>Step 10</strong> send-lifetime start-time {infinite</td>
<td>end-time</td>
</tr>
<tr>
<td><strong>Step 11</strong> end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 12</strong> show key chain</td>
<td>Display authentication key information.</td>
</tr>
<tr>
<td><strong>Step 13</strong> copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Use the no forms of these commands to disable the feature or to return the setting to the default value.
Configuring EIGRP Stub Routing

The EIGRP stub routing feature reduces resource utilization by moving routed traffic closer to the end user.

**Note**

EIGRP stub routing only advertises connected or summary routes from the routing tables to other switches in the network. The switch uses EIGRP stub routing at the access layer to eliminate the need for other types of routing advertisements. If you try to configure multi-VRF-CE and EIGRP stub routing at the same time, the configuration is not allowed.

In a network using EIGRP stub routing, the only allowable route for IP traffic to the user is through a switch that is configured with EIGRP stub routing. The switch sends the routed traffic to interfaces that are configured as user interfaces or are connected to other devices.

When using EIGRP stub routing, you need to configure the distribution and remote routers to use EIGRP and to configure only the switch as a stub. Only specified routes are propagated from the switch. The switch responds to all queries for summaries, connected routes, and routing updates.

Any neighbor that receives a packet informing it of the stub status does not query the stub router for any routes, and a router that has a stub peer does not query that peer. The stub router depends on the distribution router to send the proper updates to all peers.

In Figure 36-4, switch B is configured as an EIGRP stub router. Switches A and C are connected to the rest of the WAN. Switch B advertises connected, static, redistribution, and summary routes to switch A and C. Switch B does not advertise any routes learned from switch A (and the reverse).

![Figure 36-4 EIGRP Stub Router Configuration](image)

Beginning in privileged EXEC mode, follow these steps to configure a remote or spoke router for EIGRP stub routing:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>router eigrp 1</td>
<td>Configure a remote or distribution router to run an EIGRP process and enter router configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>network network-number</td>
<td>Associate networks with an EIGRP routing process.</td>
</tr>
</tbody>
</table>
| Step 4 | eigrp stub [receive-only | connected | static | summary] | Configure a remote router as an EIGRP stub router. The keywords have these meanings:  
  - Enter receive-only to set the router as a receive-only neighbor.  
  - Enter connected to advertise connected routes.  
  - Enter static to advertise static routes.  
  - Enter summary to advertise summary routes. |
| Step 5 | end                                           | Return to privileged EXEC mode.                                          |
| Step 6 | show ip eigrp neighbor detail               | Verify that a remote router has been configured as a stub router with EIGRP. The last line of the output shows the stub status of the remote or spoke router. |
| Step 7 | copy running-config startup-config          | (Optional) Save your entries in the configuration file.                 |

Enter the `show ip eigrp neighbor detail` privileged EXEC command from the distribution router to verify the configuration.

**Monitoring and Maintaining EIGRP**

You can delete neighbors from the neighbor table. You can also display various EIGRP routing statistics. Table 36-8 lists the privileged EXEC commands for deleting neighbors and displaying statistics. For explanations of fields in the resulting display, see the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2*.

**Table 36-8 IP EIGRP Clear and Show Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip eigrp neighbors [if-address</td>
<td>interface]</td>
</tr>
<tr>
<td>show ip eigrp interface [interface] [as number]</td>
<td>Display information about interfaces configured for EIGRP.</td>
</tr>
<tr>
<td>show ip eigrp neighbors [type-number]</td>
<td>Display EIGRP discovered neighbors.</td>
</tr>
<tr>
<td>show ip eigrp topology [autonomous-system-number]</td>
<td>Display the EIGRP topology table for a given process.</td>
</tr>
<tr>
<td>[ip-address] [mask]]</td>
<td></td>
</tr>
<tr>
<td>show ip eigrp traffic [autonomous-system-number]</td>
<td>Display the number of packets sent and received for all or a specified EIGRP process.</td>
</tr>
</tbody>
</table>
Configuring BGP

The Border Gateway Protocol (BGP) is an exterior gateway protocol used to set up an interdomain routing system that guarantees the loop-free exchange of routing information between autonomous systems. Autonomous systems are made up of routers that operate under the same administration and that run Interior Gateway Protocols (IGPs), such as RIP or OSPF, within their boundaries and that interconnect by using an Exterior Gateway Protocol (EGP). BGP Version 4 is the standard EGP for interdomain routing in the Internet. The protocol is defined in RFCs 1163, 1267, and 1771. You can find detailed information about BGP in Internet Routing Architectures, published by Cisco Press, and in the “Configuring BGP” chapter in the Cisco IOS IP and IP Routing Configuration Guide.

Note

For details about BGP commands and keywords, see the Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2. For a list of BGP commands that are visible but not supported by the switch, see Appendix C, “Unsupported Commands in Cisco IOS Release 12.2(55)SE.”

Routers that belong to the same autonomous system (AS) and that exchange BGP updates run internal BGP (IBGP), and routers that belong to different autonomous systems and that exchange BGP updates run external BGP (EBGP). Most configuration commands are the same for configuring EBGP and IBGP. The difference is that the routing updates are exchanged either between autonomous systems (EBGP) or within an AS (IBGP). Figure 36-5 shows a network that is running both EBGP and IBGP.

Before exchanging information with an external AS, BGP ensures that networks within the AS can be reached by defining internal BGP peering among routers within the AS and by redistributing BGP routing information to IGPs that run within the AS, such as IGRP and OSPF.

Routers that run a BGP routing process are often referred to as BGP speakers. BGP uses the Transmission Control Protocol (TCP) as its transport protocol (specifically port 179). Two BGP speakers that have a TCP connection to each other for exchanging routing information are known as peers or neighbors. In Figure 36-5, Routers A and B are BGP peers, as are Routers B and C and Routers C and D. The routing information is a series of AS numbers that describe the full path to the destination network. BGP uses this information to construct a loop-free map of autonomous systems.
The network has these characteristics:

- Routers A and B are running EBGP, and Routers B and C are running IBGP. Note that the EBGP peers are directly connected and that the IBGP peers are not. As long as there is an IGP running that allows the two neighbors to reach one another, IBGP peers do not have to be directly connected.

- All BGP speakers within an AS must establish a peer relationship with each other. That is, the BGP speakers within an AS must be fully meshed logically. BGP4 provides two techniques that reduce the requirement for a logical full mesh: confederations and route reflectors.

- AS 200 is a transit AS for AS 100 and AS 300—that is, AS 200 is used to transfer packets between AS 100 and AS 300.

BGP peers initially exchange their full BGP routing tables and then send only incremental updates. BGP peers also exchange keepalive messages (to ensure that the connection is up) and notification messages (in response to errors or special conditions).

In BGP, each route consists of a network number, a list of autonomous systems that information has passed through (the autonomous system path), and a list of other path attributes. The primary function of a BGP system is to exchange network reachability information, including information about the list of AS paths, with other BGP systems. This information can be used to determine AS connectivity, to prune routing loops, and to enforce AS-level policy decisions.

A router or switch running Cisco IOS does not select or use an IBGP route unless it has a route available to the next-hop router and it has received synchronization from an IGP (unless IGP synchronization is disabled). When multiple routes are available, BGP bases its path selection on attribute values. See the “Configuring BGP Decision Attributes” section on page 36-51 for information about BGP attributes.

BGP Version 4 supports classless interdomain routing (CIDR) so you can reduce the size of your routing tables by creating aggregate routes, resulting in supernets. CIDR eliminates the concept of network classes within BGP and supports the advertising of IP prefixes.

These sections briefly describe how to configure BGP and supported BGP features:

- Default BGP Configuration, page 36-45
- Enabling BGP Routing, page 36-47
- Managing Routing Policy Changes, page 36-50
- Configuring BGP Decision Attributes, page 36-51
- Configuring BGP Filtering with Route Maps, page 36-53
- Configuring BGP Filtering by Neighbor, page 36-54
- Configuring Prefix Lists for BGP Filtering, page 36-55
- Configuring BGP Community Filtering, page 36-56
- Configuring BGP Neighbors and Peer Groups, page 36-57
- Configuring Aggregate Addresses, page 36-59
- Configuring Routing Domain Confederations, page 36-60
- Configuring BGP Route Reflectors, page 36-61
- Configuring Route Dampening, page 36-62
- Monitoring and Maintaining BGP, page 36-63

For detailed descriptions of BGP configuration, see the “Configuring BGP” chapter in the Cisco IOS IP Configuration Guide, Release 12.2. For details about specific commands, see the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2*. 
For a list of BGP commands that are visible but not supported by the switch, see Appendix C, “Unsupported Commands in Cisco IOS Release12.2(55)SE.”

Default BGP Configuration

Table 36-9 shows the basic default BGP configuration. For the defaults for all characteristics, see the specific commands in the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2*.

Table 36-9  Default BGP Configuration

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aggregate address</td>
<td>Disabled: None defined.</td>
</tr>
<tr>
<td>AS path access list</td>
<td>None defined.</td>
</tr>
<tr>
<td>Auto summary</td>
<td>Enabled.</td>
</tr>
</tbody>
</table>
| Best path                    | The router considers *as-path* in choosing a route and does not compare similar routes from external BGP peers.  
                               | Compare router ID: Disabled.                                                     |
| BGP community list           | Number: None defined. When you permit a value for the community number, the list defaults to an implicit deny for everything else that has not been permitted.  
                               | Format: Cisco default format (32-bit number).                                    |
| BGP confederation identifier/peers | Identifier: None configured.  
                               | Peers: None identified.                                                          |
| BGP Fast external fallover   | Enabled.                                                                         |
| BGP local preference         | 100. The range is 0 to 4294967295 with the higher value preferred.              |
| BGP network                  | None specified; no backdoor route advertised.                                    |
| BGP route dampening          | Disabled by default. When enabled:  
                               | • Half-life is 15 minutes.                                                        |
                               | • Re-use is 750 (10-second increments).                                          |
                               | • Suppress is 2000 (10-second increments).                                      |
                               | • Max-suppress-time is 4 times half-life; 60 minutes.                           |
| BGP router ID                | The IP address of a loopback interface if one is configured or the highest IP address configured for a physical interface on the router. |
| Default information originate (protocol or network redistribution) | Disabled.                                                                      |
| Default metric               | Built-in, automatic metric translations.                                        |
| Distance                     | External route administrative distance: 20 (acceptable values are from 1 to 255).  
                               | Internal route administrative distance: 200 (acceptable values are from 1 to 255).  
                               | Local route administrative distance: 200 (acceptable values are from 1 to 255).   |
| Distribute list              | In (filter networks received in updates): Disabled.                             |
                               | Out (suppress networks from being advertised in updates): Disabled.              |
### Table 36-9  Default BGP Configuration (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal route redistribution</td>
<td>Disabled.</td>
</tr>
<tr>
<td>IP prefix list</td>
<td>None defined.</td>
</tr>
</tbody>
</table>
| Multi exit discriminator (MED)   | Always compare: Disabled. Does not compare MEDs for paths from neighbors in different autonomous systems.  
    | Best path compare: Disabled.                                                    
    | MED missing as worst path: Disabled.                                            
    | Deterministic MED comparison is disabled.                                       |
| Neighbor                         | These are default neighbor settings:                                            |
|                                  |  • Advertisement interval: 30 seconds for external peers; 5 seconds for internal peers.  
    |  • Change logging: Enabled.                                                    |
|                                  |  • Conditional advertisement: Disabled.                                          |
|                                  |  • Default originate: No default route is sent to the neighbor.                 |
|                                  |  • Description: None.                                                           |
|                                  |  • Distribute list: None defined.                                               |
|                                  |  • External BGP multihop: Only directly connected neighbors are allowed.        |
|                                  |  • Filter list: None used.                                                      |
|                                  |  • Maximum number of prefixes received: No limit.                                |
|                                  |  • Next hop (router as next hop for BGP neighbor): Disabled.                    |
|                                  |  • Password: Disabled.                                                          |
|                                  |  • Peer group: None defined; no members assigned.                                |
|                                  |  • Prefix list: None specified.                                                 |
|                                  |  • Remote AS (add entry to neighbor BGP table): No peers defined.               |
|                                  |  • Private AS number removal: Disabled.                                          |
|                                  |  • Route maps: None applied to a peer.                                           |
|                                  |  • Send community attributes: None sent to neighbors.                           |
|                                  |  • Shutdown or soft reconfiguration: Not enabled.                               |
|                                  |  • Timers: keepalive: 60 seconds; holdtime: 180 seconds.                         |
|                                  |  • Update source: Best local address.                                            |
|                                  |  • Weight: Routes learned through BGP peer: 0; routes sourced by the local router:  
    |  32768.                                                                        |
| NSF awareness                    | Disabled\(^1\). Allows Layer 3 switches to continue forwarding packets from a neighboring NSF-capable router during hardware or software changes. |
| Route reflector                  | None configured.                                                                |
| Synchronization (BGP and IGP)    | Enabled.                                                                        |
To enable this feature with BGP routing, you need to enable Graceful Restart. When the neighboring router is NSF-capable, and this feature is enabled, the Layer 3 switch continues to forward packets from the neighboring router during the interval between the primary Route Processor (RP) in a router failing and the backup RP taking over, or while the primary RP is manually reloaded for a nondisruptive software upgrade.

For more information, see the BGP Nonstop Forwarding (NSF) Awareness Feature Guide at this URL: http://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/ftbgpnsf.html

Enabling BGP Routing

To enable BGP routing, you establish a BGP routing process and define the local network. Because BGP must completely recognize the relationships with its neighbors, you must also specify a BGP neighbor. BGP supports two kinds of neighbors: internal and external. Internal neighbors are in the same AS; external neighbors are in different autonomous systems. External neighbors are usually adjacent to each other and share a subnet, but internal neighbors can be anywhere in the same AS.

The switch supports the use of private AS numbers, usually assigned by service providers and given to systems whose routes are not advertised to external neighbors. The private AS numbers are from 64512 to 65535. You can configure external neighbors to remove private AS numbers from the AS path by using the neighbor remove-private-as router configuration command. Then when an update is passed to an external neighbor, if the AS path includes private AS numbers, these numbers are dropped.

If your AS will be passing traffic through it from another AS to a third AS, it is important to be consistent about the routes it advertises. If BGP advertised a route before all routers in the network had learned about the route through the IGP, the AS might receive traffic that some routers could not yet route. To prevent this from happening, BGP must wait until the IGP has propagated information across the AS so that BGP is synchronized with the IGP. Synchronization is enabled by default. If your AS does not pass traffic from one AS to another AS, or if all routers in your autonomous systems are running BGP, you can disable synchronization, which allows your network to carry fewer routes in the IGP and allows BGP to converge more quickly.

Beginning in privileged EXEC mode, follow these steps to enable BGP routing, establish a BGP routing process, and specify a neighbor:
### Command Purpose

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>ip routing</td>
<td>Enable IP routing (required only if IP routing is disabled).</td>
</tr>
<tr>
<td>3</td>
<td>router bgp autonomous-system</td>
<td>Enable a BGP routing process, assign it an AS number, and enter router configuration mode. The AS number can be from 1 to 65535, with 64512 to 65535 designated as private autonomous numbers.</td>
</tr>
<tr>
<td>4</td>
<td>network network-number [mask network-mask] [route-map route-map-name]</td>
<td>Configure a network as local to this AS, and enter it in the BGP table.</td>
</tr>
<tr>
<td>5</td>
<td>neighbor [ip-address</td>
<td>peer-group-name] remote-as number</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For EBGP, neighbors are usually directly connected, and the IP address is the address of the interface at the other end of the connection.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For IBGP, the IP address can be the address of any of the router interfaces.</td>
</tr>
<tr>
<td>6</td>
<td>neighbor [ip-address</td>
<td>peer-group-name] remove-private-as</td>
</tr>
<tr>
<td>7</td>
<td>no synchronization</td>
<td>(Optional) Disable synchronization between BGP and an IGP.</td>
</tr>
<tr>
<td>8</td>
<td>no auto-summary</td>
<td>(Optional) Disable automatic network summarization. By default, when a subnet is redistributed from an IGP into BGP, only the network route is inserted into the BGP table.</td>
</tr>
<tr>
<td>9</td>
<td>bgp fast-external-fallover</td>
<td>(Optional) Automatically reset a BGP session when a link between external neighbors goes down. By default, the session is not immediately reset.</td>
</tr>
<tr>
<td>10</td>
<td>bgp graceful-restart</td>
<td>(Optional) Enable NSF awareness on switch. By default, NSF awareness is disabled.</td>
</tr>
<tr>
<td>11</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>12</td>
<td>show ip bgp network network-number</td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td></td>
<td>or</td>
<td>Verify that NSF awareness (Graceful Restart) is enabled on the neighbor.</td>
</tr>
<tr>
<td></td>
<td>show ip bgp neighbor</td>
<td>If NSF awareness is enabled on the switch and the neighbor, this message appears:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Graceful Restart Capability: advertised and received</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If NSF awareness is enabled on the switch, but not on the neighbor, this message appears:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Graceful Restart Capability: advertised</td>
</tr>
<tr>
<td>13</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
Use the `no router bgp autonomous-system` global configuration command to remove a BGP AS. Use the `no network network-number` router configuration command to remove the network from the BGP table. Use the `no neighbor {ip-address | peer-group-name} remote-as number` router configuration command to remove a neighbor. Use the `no neighbor {ip-address | peer-group-name} remove-private-as` router configuration command to include private AS numbers in updates to a neighbor. Use the `synchronization` router configuration command to re-enable synchronization.

These examples show how to configure BGP on the routers in Figure 36-5.

**Router A:**

Switch(config)# router bgp 100
Switch(config-router)# neighbor 129.213.1.1 remote-as 200

**Router B:**

Switch(config)# router bgp 200
Switch(config-router)# neighbor 129.213.1.2 remote-as 100
Switch(config-router)# neighbor 175.220.1.2 remote-as 200

**Router C:**

Switch(config)# router bgp 200
Switch(config-router)# neighbor 175.220.212.1 remote-as 200
Switch(config-router)# neighbor 192.208.10.1 remote-as 300

**Router D:**

Switch(config)# router bgp 300
Switch(config-router)# neighbor 192.208.10.2 remote-as 200

To verify that BGP peers are running, use the `show ip bgp neighbors` privileged EXEC command. This is the output of this command on Router A:

Switch# show ip bgp neighbors

BGP neighbor is 129.213.1.1, remote AS 200, external link
BGP version 4, remote router ID 175.220.212.1
BGP state = established, table version = 3, up for 0:10:59
Last read 0:00:29, hold time is 180, keepalive interval is 60 seconds
Minimum time between advertisement runs is 30 seconds
Received 2828 messages, 0 notifications, 0 in queue
Sent 2826 messages, 0 notifications, 0 in queue
Connections established 11; dropped 10

Anything other than `state = established` means that the peers are not running. The remote router ID is the highest IP address on that router (or the highest loopback interface). Each time the table is updated with new information, the table version number increments. A table version number that continually increments means that a route is flapping, causing continual routing updates.

For exterior protocols, a reference to an IP network from the `network` router configuration command controls only which networks are advertised. This is in contrast to Interior Gateway Protocols (IGPs), such as EIGRP, which also use the `network` command to determine where to send updates.

For detailed descriptions of BGP configuration, see the “IP Routing Protocols” chapter in the *Cisco IOS IP Configuration Guide, Release 12.2*. For details about specific commands, see the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2*. See Appendix C, “Unsupported Commands in Cisco IOS Release12.2(55)SE,” for a list of BGP commands that are visible but not supported by the switch.
Managing Routing Policy Changes

Routing policies for a peer include all the configurations that might affect inbound or outbound routing table updates. When you have defined two routers as BGP neighbors, they form a BGP connection and exchange routing information. If you later change a BGP filter, weight, distance, version, or timer, or make a similar configuration change, you must reset the BGP sessions so that the configuration changes take effect.

There are two types of reset, hard reset and soft reset. Cisco IOS software releases 12.1 and later support a soft reset without any prior configuration. To use a soft reset without preconfiguration, both BGP peers must support the soft route refresh capability, which is advertised in the OPEN message sent when the peers establish a TCP session. A soft reset allows the dynamic exchange of route refresh requests and routing information between BGP routers and the subsequent re-advertisement of the respective outbound routing table.

- When soft reset generates inbound updates from a neighbor, it is called dynamic inbound soft reset.
- When soft reset sends a set of updates to a neighbor, it is called outbound soft reset.

A soft inbound reset causes the new inbound policy to take effect. A soft outbound reset causes the new local outbound policy to take effect without resetting the BGP session. As a new set of updates is sent during outbound policy reset, a new inbound policy can also take effect.

Table 36-10 lists the advantages and disadvantages hard reset and soft reset.

<table>
<thead>
<tr>
<th>Type of Reset</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hard reset</td>
<td>No memory overhead</td>
<td>The prefixes in the BGP, IP, and FIB tables provided by the neighbor are lost. Not recommended.</td>
</tr>
<tr>
<td>Outbound soft reset</td>
<td>No configuration, no storing of routing table updates</td>
<td>Does not reset inbound routing table updates.</td>
</tr>
<tr>
<td>Dynamic inbound soft reset</td>
<td>Does not clear the BGP session and cache routing table updates and has no memory overhead</td>
<td>Both BGP routers must support the route refresh capability (in Cisco IOS Release 12.1 and later).</td>
</tr>
</tbody>
</table>

Beginning in privileged EXEC mode, follow these steps to determine if a BGP peer supports the route refresh capability and to reset the BGP session:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><strong>show ip bgp neighbors</strong></td>
<td>Display whether a neighbor supports the route refresh capability. When supported, this message appears for the router: Received route refresh capability from peer.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>clear ip bgp</td>
<td>Reset the routing table on the specified connection.</td>
</tr>
<tr>
<td>[*] address</td>
<td>• Enter an asterisk (*) to specify that all connections be reset.</td>
</tr>
<tr>
<td>peer-group-name</td>
<td>• Enter an IP address to specify the connection to be reset.</td>
</tr>
<tr>
<td></td>
<td>• Enter a peer group name to reset the peer group.</td>
</tr>
</tbody>
</table>
When a BGP speaker receives updates from multiple autonomous systems that describe different paths to the same destination, it must choose the single best path for reaching that destination. When chosen, the selected path is entered into the BGP routing table and propagated to its neighbors. The decision is based on the value of attributes that the update contains and other BGP-configurable factors.

When a BGP peer learns two EBGP paths for a prefix from a neighboring AS, it chooses the best path and inserts that path in the IP routing table. If BGP multipath support is enabled and the EBGP paths are learned from the same neighboring autonomous systems, instead of a single best path, multiple paths are installed in the IP routing table. Then, during packet switching, per-packet or per-destination load balancing is performed among the multiple paths. The maximum-paths router configuration command controls the number of paths allowed.

These factors summarize the order in which BGP evaluates the attributes for choosing the best path:

1. If the path specifies a next hop that is inaccessible, drop the update. The BGP next-hop attribute, automatically determined by the software, is the IP address of the next hop that is going to be used to reach a destination. For EBGP, this is usually the IP address of the neighbor specified by the neighbor remote-as router configuration command. You can disable next-hop processing by using route maps or the neighbor next-hop-self router configuration command.

2. Prefer the path with the largest weight (a Cisco proprietary parameter). The weight attribute is local to the router and not propagated in routing updates. By default, the weight attribute is 32768 for paths that the router originates and zero for other paths. Routes with the largest weight are preferred. You can use access lists, route maps, or the neighbor weight router configuration command to set weights.

3. Prefer the route with the highest local preference. Local preference is part of the routing update and exchanged among routers in the same AS. The default value of the local preference attribute is 100. You can set local preference by using the bgp default local-preference router configuration command or by using a route map.

4. Prefer the route that was originated by BGP running on the local router.

5. Prefer the route with the shortest AS path.

6. Prefer the route with the lowest origin type. An interior route or IGP is lower than a route learned by EGP, and an EGP-learned route is lower than one of unknown origin or learned in another way.

7. Prefer the route with the lowest multi-exit discriminator (MED) metric attribute if the neighboring AS is the same for all routes considered. You can configure the MED by using route maps or by using the default-metric router configuration command. When an update is sent to an IBGP peer, the MED is included.

8. Prefer the external (EBGP) path over the internal (IBGP) path.

### Configuring BGP Decision Attributes

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong> clear ip bgp { *</td>
<td>address</td>
</tr>
</tbody>
</table>
| **Step 4** show ip bgp 
show ip bgp neighbors | Verify the reset by checking information about the routing table and about BGP neighbors. |
9. Prefer the route that can be reached through the closest IGP neighbor (the lowest IGP metric). This means that the router will prefer the shortest internal path within the AS to reach the destination (the shortest path to the BGP next-hop).

10. If the following conditions are all true, insert the route for this path into the IP routing table:
   - Both the best route and this route are external.
   - Both the best route and this route are from the same neighboring autonomous system.
   - maximum-paths is enabled.

11. If multipath is not enabled, prefer the route with the lowest IP address value for the BGP router ID. The router ID is usually the highest IP address on the router or the loopback (virtual) address, but might be implementation-specific.

Beginning in privileged EXEC mode, follow these steps to configure some decision attributes:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>router bgp autonomous-system</td>
</tr>
<tr>
<td>Step 3</td>
<td>bgp best-path as-path ignore</td>
</tr>
<tr>
<td>Step 4</td>
<td>neighbor {ip-address</td>
</tr>
<tr>
<td>Step 5</td>
<td>neighbor {ip-address</td>
</tr>
<tr>
<td>Step 6</td>
<td>default-metric number</td>
</tr>
<tr>
<td>Step 7</td>
<td>bgp bestpath med missing-as-worst</td>
</tr>
<tr>
<td>Step 8</td>
<td>bgp always-compare med</td>
</tr>
<tr>
<td>Step 9</td>
<td>bgp bestpath med confed</td>
</tr>
<tr>
<td>Step 10</td>
<td>bgp deterministic med</td>
</tr>
</tbody>
</table>
### Configuring BGP Filtering with Route Maps

Within BGP, route maps can be used to control and to modify routing information and to define the conditions by which routes are redistributed between routing domains. See the “Using Route Maps to Redistribute Routing Information” section on page 36-102 for more information about route maps. Each route map has a name that identifies the route map (map tag) and an optional sequence number.

Beginning in privileged EXEC mode, follow these steps to use a route map to disable next-hop processing:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>route-map map-tag [[permit</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>set ip next-hop ip-address [...ip-address] [peer-address]</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>show route-map [map-name]</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

Use the **no** form of each command to return to the default state.

### Configuring BGP Filtering with Route Maps

Use the **no route-map map-tag** command to delete the route map. Use the **no set ip next-hop ip-address** command to re-enable next-hop processing.
Configuring BGP Filtering by Neighbor

You can filter BGP advertisements by using AS-path filters, such as the `as-path access-list` global configuration command and the `neighbor filter-list` router configuration command. You can also use access lists with the `neighbor distribute-list` router configuration command. Distribute-list filters are applied to network numbers. See the “Controlling Advertising and Processing in Routing Updates” section on page 36-110 for information about the `distribute-list` command.

You can use route maps on a per-neighbor basis to filter updates and to modify various attributes. A route map can be applied to either inbound or outbound updates. Only the routes that pass the route map are sent or accepted in updates. On both inbound and outbound updates, matching is supported based on AS path, community, and network numbers. Autonomous system path matching requires the `match as-path` route-map command, community based matching requires the `match community-list` route-map command, and network-based matching requires the `ip access-list` global configuration command.

Beginning in privileged EXEC mode, follow these steps to apply a per-neighbor route map:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>router bgp autonomous-system</td>
</tr>
<tr>
<td>Step 3</td>
<td>neighbor {ip-address \ peer-group name} distribute-list {access-list-number \ name} [in \ out]</td>
</tr>
<tr>
<td>Step 4</td>
<td>neighbor {ip-address \ peer-group name} route-map map-tag [in \ out]</td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
</tr>
<tr>
<td>Step 6</td>
<td>show ip bgp neighbors</td>
</tr>
<tr>
<td>Step 7</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

Use the `no neighbor distribute-list` command to remove the access list from the neighbor. Use the `no neighbor route-map map-tag` router configuration command to remove the route map from the neighbor.

Another method of filtering is to specify an access list filter on both incoming and outbound updates, based on the BGP autonomous system paths. Each filter is an access list based on regular expressions. (For more information on forming regular expressions, see the “Regular Expressions” appendix in the *Cisco IOS Dial Services Command Reference.*) To use this method, define an autonomous system path access list, and apply it to updates to and from particular neighbors.

Beginning in privileged EXEC mode, follow these steps to configure BGP path filtering:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip as-path access-list access-list-number [permit \ deny] as-regular-expressions</td>
</tr>
</tbody>
</table>
### Configuring Prefix Lists for BGP Filtering

You can use prefix lists as an alternative to access lists in many BGP route filtering commands, including the `neighbor distribute-list` router configuration command. The advantages of using prefix lists include performance improvements in loading and lookup of large lists, incremental update support, easier CLI configuration, and greater flexibility.

Filtering by a prefix list involves matching the prefixes of routes with those listed in the prefix list, as when matching access lists. When there is a match, the route is used. Whether a prefix is permitted or denied is based upon these rules:

- An empty prefix list permits all prefixes.
- An implicit deny is assumed if a given prefix does not match any entries in a prefix list.
- When multiple entries of a prefix list match a given prefix, the sequence number of a prefix list entry identifies the entry with the lowest sequence number.

By default, sequence numbers are generated automatically and incremented in units of five. If you disable the automatic generation of sequence numbers, you must specify the sequence number for each entry. You can specify sequence values in any increment. If you specify increments of one, you cannot insert additional entries into the list; if you choose very large increments, you might run out of values.

You do not need to specify a sequence number when removing a configuration entry. `Show` commands include the sequence numbers in their output.

Before using a prefix list in a command, you must set up the prefix list. Beginning in privileged EXEC mode, follow these steps to create a prefix list or to add an entry to a prefix list:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 ip prefix-list list-name seq seq-value deny</td>
<td>Create a prefix list with an optional sequence number to deny or permit access for matching conditions. You must enter at least one permit or deny clause.</td>
</tr>
<tr>
<td>Step 3 ip prefix-list list-name seq seq-value deny</td>
<td>Add an entry to a prefix list, and assign a sequence number to the entry.</td>
</tr>
<tr>
<td>Step 3 ip prefix-list list-name seq seq-value deny</td>
<td>Add an entry to a prefix list, and assign a sequence number to the entry.</td>
</tr>
</tbody>
</table>
Configuring BGP Community Filtering

One way that BGP controls the distribution of routing information based on the value of the COMMUNITIES attribute. The attribute is a way to group destinations into communities and to apply routing decisions based on the communities. This method simplifies configuration of a BGP speaker to control distribution of routing information.

A community is a group of destinations that share some common attribute. Each destination can belong to multiple communities. AS administrators can define to which communities a destination belongs. By default, all destinations belong to the general Internet community. The community is identified by the COMMUNITIES attribute, an optional, transitive, global attribute in the numerical range from 1 to 4294967200. These are some predefined, well-known communities:

- **internet**—Advertise this route to the Internet community. All routers belong to it.
- **no-export**—Do not advertise this route to EBGP peers.
- **no-advertise**—Do not advertise this route to any peer (internal or external).
- **local-as**—Do not advertise this route to peers outside the local autonomous system.

Based on the community, you can control which routing information to accept, prefer, or distribute to other neighbors. A BGP speaker can set, append, or modify the community of a route when learning, advertising, or redistributing routes. When routes are aggregated, the resulting aggregate has a COMMUNITIES attribute that contains all communities from all the initial routes.

You can use community lists to create groups of communities to use in a match clause of a route map. As with an access list, a series of community lists can be created. Statements are checked until a match is found. As soon as one statement is satisfied, the test is concluded.

To set the COMMUNITIES attribute and match clauses based on communities, see the `match community-list` and `set community` route-map configuration commands in the “Using Route Maps to Redistribute Routing Information” section on page 36-102.

By default, no COMMUNITIES attribute is sent to a neighbor. You can specify that the COMMUNITIES attribute be sent to the neighbor at an IP address by using the `neighbor send-community` router configuration command.

Beginning in privileged EXEC mode, follow these steps to create and to apply a community list:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>`show ip prefix-list [detail</td>
<td>summary] name [network/len] [seq seq-num] [longer] [first-match]`</td>
</tr>
<tr>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To delete a prefix list and all of its entries, use the `no ip prefix-list list-name` global configuration command. To delete an entry from a prefix list, use the `no ip prefix-list seq seq-value` global configuration command. To disable automatic generation of sequence numbers, use the `no ip prefix-list sequence number` command; to reenable automatic generation, use the `ip prefix-list sequence number` command. To clear the hit-count table of prefix list entries, use the `clear ip prefix-list` privileged EXEC command.
Chapter 36  Configuring IP Unicast Routing

Configuring BGP

Often many BGP neighbors are configured with the same update policies (that is, the same outbound route maps, distribute lists, filter lists, update source, and so on). Neighbors with the same update policies can be grouped into peer groups to simplify configuration and to make updating more efficient. When you have configured many peers, we recommend this approach.

To configure a BGP peer group, you create the peer group, assign options to the peer group, and add neighbors as peer group members. You configure the peer group by using the neighbor router configuration commands. By default, peer group members inherit all the configuration options of the peer group, including the remote-as (if configured), version, update-source, out-route-map, out-filter-list, out-dist-list, minimum-advertisement-interval, and next-hop-self. All peer group members also inherit changes made to the peer group. Members can also be configured to override the options that do not affect outbound updates.

To assign configuration options to an individual neighbor, specify any of these router configuration commands by using the neighbor IP address. To assign the options to a peer group, specify any of the commands by using the peer group name. You can disable a BGP peer or peer group without removing all the configuration information by using the neighbor shutdown router configuration command.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>ip community-list</td>
<td>Create a community list, and assign it a number.</td>
</tr>
<tr>
<td>{permit</td>
<td>deny} community-number</td>
</tr>
<tr>
<td></td>
<td>identifies one or more permit or deny groups of communities.</td>
</tr>
<tr>
<td></td>
<td>• The community-number is the number configured by a set community</td>
</tr>
<tr>
<td></td>
<td>route-map configuration command.</td>
</tr>
<tr>
<td>router bgp autonomous-system</td>
<td>Enter BGP router configuration mode.</td>
</tr>
<tr>
<td>neighbor {ip-address</td>
<td>peer-group name} send-community</td>
</tr>
<tr>
<td></td>
<td>this IP address.</td>
</tr>
<tr>
<td>set comm-list list-num delete</td>
<td>(Optional) Remove communities from the community attribute of an</td>
</tr>
<tr>
<td></td>
<td>inbound or outbound update that match a standard or extended</td>
</tr>
<tr>
<td></td>
<td>community list specified by a route map.</td>
</tr>
<tr>
<td>exit</td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td>ip bgp-community new-format</td>
<td>(Optional) Display and parse BGP communities in the format AA:NN.</td>
</tr>
<tr>
<td></td>
<td>A BGP community is displayed in a two-part format 2 bytes long. The</td>
</tr>
<tr>
<td></td>
<td>Cisco default community format is in the format NNAA. In the most</td>
</tr>
<tr>
<td></td>
<td>recent RFC for BGP, a community takes the form AA:NN, where the</td>
</tr>
<tr>
<td></td>
<td>first part is the AS number and the second part is a 2-byte number.</td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>show ip bgp community</td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Configuring BGP Neighbors and Peer Groups
Beginning in privileged EXEC mode, use these commands to configure BGP peers:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>router bgp autonomous-system</td>
</tr>
<tr>
<td>Step 3</td>
<td>neighbor peer-group-name peer-group</td>
</tr>
<tr>
<td>Step 4</td>
<td>neighbor ip-address peer-group peer-group-name</td>
</tr>
<tr>
<td>Step 5</td>
<td>neighbor (ip-address</td>
</tr>
<tr>
<td>Step 6</td>
<td>neighbor (ip-address</td>
</tr>
<tr>
<td>Step 7</td>
<td>neighbor (ip-address</td>
</tr>
<tr>
<td>Step 8</td>
<td>neighbor (ip-address</td>
</tr>
<tr>
<td>Step 9</td>
<td>neighbor (ip-address</td>
</tr>
<tr>
<td>Step 10</td>
<td>neighbor (ip-address</td>
</tr>
<tr>
<td>Step 11</td>
<td>neighbor (ip-address</td>
</tr>
<tr>
<td>Step 12</td>
<td>neighbor (ip-address</td>
</tr>
<tr>
<td>Step 13</td>
<td>neighbor (ip-address</td>
</tr>
<tr>
<td>Step 14</td>
<td>neighbor (ip-address</td>
</tr>
<tr>
<td>Step 15</td>
<td>neighbor (ip-address</td>
</tr>
<tr>
<td>Step 16</td>
<td>neighbor (ip-address</td>
</tr>
<tr>
<td>Step 17</td>
<td>neighbor (ip-address</td>
</tr>
</tbody>
</table>
To disable an existing BGP neighbor or neighbor peer group, use the `neighbor shutdown` router configuration command. To enable a previously existing neighbor or neighbor peer group that had been disabled, use the `no neighbor shutdown` router configuration command.

### Configuring Aggregate Addresses

Classless interdomain routing (CIDR) enables you to create aggregate routes (or supernets) to minimize the size of routing tables. You can configure aggregate routes in BGP either by redistributing an aggregate route into BGP or by creating an aggregate entry in the BGP routing table. An aggregate address is added to the BGP table when there is at least one more specific entry in the BGP table.

Beginning in privileged EXEC mode, use these commands to create an aggregate address in the routing table:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 <code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 <code>router bgp autonomous-system</code></td>
<td>Enter BGP router configuration mode.</td>
</tr>
<tr>
<td>Step 3 <code>aggregate-address address mask</code></td>
<td>Create an aggregate entry in the BGP routing table. The aggregate route is advertised as coming from the AS, and the atomic aggregate attribute is set to indicate that information might be missing.</td>
</tr>
</tbody>
</table>
Configuring BGP

To delete an aggregate entry, use the **no aggregate-address address mask** router configuration command. To return options to the default values, use the command with keywords.

### Configuring Routing Domain Confederations

One way to reduce the IBGP mesh is to divide an autonomous system into multiple subautonomous systems and to group them into a single confederation that appears as a single autonomous system. Each autonomous system is fully meshed within itself and has a few connections to other autonomous systems in the same confederation. Even though the peers in different autonomous systems have EBGP sessions, they exchange routing information as if they were IBGP peers. Specifically, the next hop, MED, and local preference information is preserved. You can then use a single IGP for all of the autonomous systems.

To configure a BGP confederation, you must specify a confederation identifier that acts as the autonomous system number for the group of autonomous systems.

Beginning in privileged EXEC mode, use these commands to configure a BGP confederation:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>router bgp autonomous-system</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>bgp confederation identifier autonomous-system</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>bgp confederation peers autonomous-system [autonomous-system ...]</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>end</td>
</tr>
</tbody>
</table>
Configuring BGP Route Reflectors

BGP requires that all of the IBGP speakers be fully meshed. When a router receives a route from an external neighbor, it must advertise it to all internal neighbors. To prevent a routing information loop, all IBPG speakers must be connected. The internal neighbors do not send routes learned from internal neighbors to other internal neighbors.

With route reflectors, all IBGP speakers need not be fully meshed because another method is used to pass learned routes to neighbors. When you configure an internal BGP peer to be a route reflector, it is responsible for passing IBGP learned routes to a set of IBGP neighbors. The internal peers of the route reflector are divided into two groups: client peers and nonclient peers (all the other routers in the autonomous system). A route reflector reflects routes between these two groups. The route reflector and its client peers form a cluster. The nonclient peers must be fully meshed with each other, but the client peers need not be fully meshed. The clients in the cluster do not communicate with IBGP speakers outside their cluster.

When the route reflector receives an advertised route, it takes one of these actions, depending on the neighbor:

- A route from an external BGP speaker is advertised to all clients and nonclient peers.
- A route from a nonclient peer is advertised to all clients.
- A route from a client is advertised to all clients and nonclient peers. Hence, the clients need not be fully meshed.

Usually a cluster of clients have a single route reflector, and the cluster is identified by the route reflector router ID. To increase redundancy and to avoid a single point of failure, a cluster might have more than one route reflector. In this case, all route reflectors in the cluster must be configured with the same 4-byte cluster ID so that a route reflector can recognize updates from route reflectors in the same cluster. All the route reflectors serving a cluster should be fully meshed and should have identical sets of client and nonclient peers.

Beginning in privileged EXEC mode, use these commands to configure a route reflector and clients:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>router bgp autonomous-system</td>
</tr>
<tr>
<td>Step 3</td>
<td>neighbor ip-address</td>
</tr>
<tr>
<td>Step 4</td>
<td>bgp cluster-id cluster-id</td>
</tr>
<tr>
<td>Step 5</td>
<td>no bgp client-to-client reflection</td>
</tr>
</tbody>
</table>
Chapter 36  Configuring IP Unicast Routing

Configuring Route Dampening

Route flap dampening is a BGP feature designed to minimize the propagation of flapping routes across an internetwork. A route is considered to be flapping when it is repeatedly available, then unavailable, then available, then unavailable, and so on. When route dampening is enabled, a numeric penalty value is assigned to a route when it flaps. When a route’s accumulated penalties reach a configurable limit, BGP suppresses advertisements of the route, even if the route is running. The reuse limit is a configurable value that is compared with the penalty. If the penalty is less than the reuse limit, a suppressed route that is up is advertised again.

Dampening is not applied to routes that are learned by IBGP. This policy prevents the IBGP peers from having a higher penalty for routes external to the AS.

Beginning in privileged EXEC mode, use these commands to configure BGP route dampening:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>router bgp autonomous-system</td>
</tr>
<tr>
<td>Step 3</td>
<td>bgp dampening</td>
</tr>
<tr>
<td>Step 4</td>
<td>bgp dampening half-life reuse suppress max-suppress [route-map map]</td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
</tr>
<tr>
<td>Step 6</td>
<td>show ip bgp flap-statistics [{regexp regex}</td>
</tr>
<tr>
<td></td>
<td>[filter-list list]</td>
</tr>
<tr>
<td></td>
<td>[address mask [longer-prefix]]</td>
</tr>
<tr>
<td>Step 7</td>
<td>show ip bgp dampened-paths</td>
</tr>
<tr>
<td>Step 8</td>
<td>clear ip bgp flap-statistics [{regexp regex}</td>
</tr>
<tr>
<td></td>
<td>[filter-list list]</td>
</tr>
<tr>
<td></td>
<td>[address mask [longer-prefix]]</td>
</tr>
<tr>
<td>Step 9</td>
<td>clear ip bgp dampening</td>
</tr>
<tr>
<td>Step 10</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To disable flap dampening, use the no bgp dampening router configuration command without keywords. To set dampening factors back to the default values, use the no bgp dampening router configuration command with values.
Monitoring and Maintaining BGP

You can remove all contents of a particular cache, table, or database. This might be necessary when the contents of the particular structure have become or are suspected to be invalid.

You can display specific statistics, such as the contents of BGP routing tables, caches, and databases. You can use the information to determine resource utilization and solve network problems. You can also display information about node reachability and discover the routing path your device’s packets are taking through the network.

Table 36-8 lists the privileged EXEC commands for clearing and displaying BGP. For explanations of the display fields, see the Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2.

Table 36-11  IP BGP Clear and Show Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip bgp address</td>
<td>Reset a particular BGP connection.</td>
</tr>
<tr>
<td>clear ip bgp *</td>
<td>Reset all BGP connections.</td>
</tr>
<tr>
<td>clear ip bgp peer-group tag</td>
<td>Remove all members of a BGP peer group.</td>
</tr>
<tr>
<td>show ip bgp prefix</td>
<td>Display peer groups and peers not in peer groups to which the prefix has been advertised. Also display prefix attributes such as the next hop and the local prefix.</td>
</tr>
<tr>
<td>show ip bgp cidr-only</td>
<td>Display all BGP routes that contain subnet and supernet network masks.</td>
</tr>
<tr>
<td>show ip bgp community community-number exact</td>
<td>Display routes that belong to the specified communities.</td>
</tr>
<tr>
<td>show ip bgp community-list community-list-number [exact-match]</td>
<td>Display routes that are permitted by the community list.</td>
</tr>
<tr>
<td>show ip bgp filter-list access-list-number</td>
<td>Display routes that are matched by the specified AS path access list.</td>
</tr>
<tr>
<td>show ip bgp inconsistent-as</td>
<td>Display the routes with inconsistent originating autonomous systems.</td>
</tr>
<tr>
<td>show ip bgp regexp regular-expression</td>
<td>Display the routes that have an AS path that matches the specified regular expression entered on the command line.</td>
</tr>
<tr>
<td>show ip bgp</td>
<td>Display the contents of the BGP routing table.</td>
</tr>
<tr>
<td>show ip bgp neighbors [address]</td>
<td>Display detailed information on the BGP and TCP connections to individual neighbors.</td>
</tr>
<tr>
<td>show ip bgp neighbors [address] advertised-routes dampened-routes flap-statistics paths regular-expression received-routes routes</td>
<td>Display routes learned from a particular BGP neighbor.</td>
</tr>
<tr>
<td>show ip bgp paths</td>
<td>Display all BGP paths in the database.</td>
</tr>
<tr>
<td>show ip bgp peer-group [tag] [summary]</td>
<td>Display information about BGP peer groups.</td>
</tr>
<tr>
<td>show ip bgp summary</td>
<td>Display the status of all BGP connections.</td>
</tr>
</tbody>
</table>

You can also enable the logging of messages generated when a BGP neighbor resets, comes up, or goes down by using the bgp log-neighbor changes router configuration command.
Configuring ISO CLNS Routing

The International Organization for Standardization (ISO) Connectionless Network Service (CLNS) protocol is a standard for the network layer of the Open System Interconnection (OSI) model. Addresses in the ISO network architecture are referred to as network service access point (NSAP) addresses and network entity titles (NETs). Each node in an OSI network has one or more NETs. In addition, each node has many NSAP addresses.

When you enable connectionless routing on the switch by using the `clns routing` global configuration command, the switch makes only forwarding decisions, with no routing-related functionality. For dynamic routing, you must also enable a routing protocol. The switch supports the Intermediate System-to-Intermediate System (IS-IS) dynamic routing protocols for ISO CLNS networks:

When dynamically routing, you use IS-IS. This routing protocol supports the concept of areas. Within an area, all routers know how to reach all the system IDs. Between areas, routers know how to reach the proper area. IS-IS supports two levels of routing: station routing (within an area) and area routing (between areas).

The key difference between the ISO IGRP and IS-IS NSAP addressing schemes is in the definition of area addresses. Both use the system ID for Level 1 routing (routing within an area). However, they differ in the way addresses are specified for area routing. An ISO IGRP NSAP address includes three separate fields for routing: the domain, area, and system ID. An IS-IS address includes two fields: a single continuous area field (comprising the domain and area fields) and the system ID.

For more detailed information about ISO CLNS, see the *Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS and XNS Configuration Guide, Release 12.2*. For complete syntax and usage information for the commands used in this chapter, see the *Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS and XNS Command Reference, Release 12.2*, use the IOS command reference master index, or search online.

Configuring IS-IS Dynamic Routing

IS-IS is an ISO dynamic routing protocol (described in ISO 105890). Unlike other routing protocols, enabling IS-IS requires that you create an IS-IS routing process and assign it to a specific interface, rather than to a network. You can specify more than one IS-IS routing process per Layer 3 switch or router by using the multiarea IS-IS configuration syntax. You then configure the parameters for each instance of the IS-IS routing process.

Small IS-IS networks are built as a single area that includes all the routers in the network. As the network grows larger, it is usually reorganized into a backbone area made up of the connected set of all Level 2 routers from all areas, which is in turn connected to local areas. Within a local area, routers know how to reach all system IDs. Between areas, routers know how to reach the backbone, and the backbone routers know how to reach other areas.

Routers establish Level 1 adjacencies to perform routing within a local area (station routing). Routers establish Level 2 adjacencies to perform routing between Level 1 areas (area routing).

A single Cisco router can participate in routing in up to 29 areas and can perform Level 2 routing in the backbone. In general, each routing process corresponds to an area. By default, the first instance of the routing process configured performs both Level 1 and Level 2 routing. You can configure additional router instances, which are automatically treated as Level 1 areas. You must configure the parameters for each instance of the IS-IS routing process individually.
For IS-IS multiarea routing, you can configure only one process to perform Level 2 routing, although you can define up to 29 Level 1 areas for each Cisco unit. If Level 2 routing is configured on any process, all additional processes are automatically configured as Level 1. You can configure this process to perform Level 1 routing at the same time. If Level 2 routing is not desired for a router instance, remove the Level 2 capability using the `is-type` global configuration command. Use the `is-type` command also to configure a different router instance as a Level 2 router.

Note
For more detailed information about IS-IS, see the “IP Routing Protocols” chapter of the *Cisco IOS IP Configuration Guide, Release 12.2*. For complete syntax and usage information for the commands used in this section, see the *Cisco IOS IP Command Reference, Release 12.2*.

This section briefly describes how to configure IS-IS routing. It includes this information:

- Default IS-IS Configuration, page 36-65
- Enabling IS-IS Routing, page 36-66
- Configuring IS-IS Global Parameters, page 36-68
- Configuring IS-IS Interface Parameters, page 36-70

**Default IS-IS Configuration**

Table 36-12 shows the default IS-IS configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ignore link-state PDU (LSP) errors</td>
<td>Enabled.</td>
</tr>
</tbody>
</table>
| IS-IS type                      | Conventional IS-IS: the router acts as both a Level 1 (station) and a Level 2 (area) router.  
                                     | Multiarea IS-IS: the first instance of the IS-IS routing process is a Level 1-2 router. Remaining instances are Level 1 routers. |
| Default-information originate    | Disabled.                                                                       |
| Log IS-IS adjacency state changes | Disabled.                                                                       |
| LSP generation throttling timers | Maximum interval between two consecutive occurrences: 5 seconds. 
                                     | Initial LSP generation delay: 50 ms. 
                                     | Hold time between the first and second LSP generation: 5000 ms. |
| LSP maximum lifetime (without a refresh) | 1200 seconds (20 minutes) before the LSP packet is deleted. |
| LSP refresh interval             | Send LSP refreshes every 900 seconds (15 minutes).                              |
| Maximum LSP packet size          | 1497 bytes.                                                                    |
| NSF Awareness1                   | Enabled2. Allows Layer 3 switches to continue forwarding packets from a neighboring NSF-capable router during hardware or software changes. |
| Partial route computation (PRC) throttling timers | Maximum PRC wait interval: 5 seconds. 
                                     | Initial PRC calculation delay after a topology change: 2000 ms. 
                                     | Hold time between the first and second PRC calculation: 5000 ms. |
| Partition avoidance              | Disabled.                                                                       |
Configuring ISO CLNS Routing

Chapter 36  Configuring IP Unicast Routing

Configuring ISO CLNS Routing

The integrated IS-IS NSF Awareness feature is supported for IPv4, beginning with Cisco IOS Release 12.2(25)SEG. The feature allows customer premises equipment (CPE) routers that are NSF-aware to help NSF-capable routers perform nonstop forwarding of packets. The local router is not necessarily performing NSF, but its awareness of NSF allows the integrity and accuracy of the routing database and link-state database on the neighboring NSF-capable router to be maintained during the switchover process.

This feature is automatically enabled and requires no configuration. For more information on this feature, see the Integrated IS-IS Nonstop Forwarding (NSF) Awareness Feature Guide at this URL: http://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/isnsfawa.html

Enabling IS-IS Routing

To enable IS-IS, you specify a name and NET for each routing process. You then enable IS-IS routing on the interface and specify the area for each instance of the routing process.

Beginning in privileged EXEC mode, follow these steps to enable IS-IS and specify the area for each instance of the IS-IS routing process:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td></td>
</tr>
<tr>
<td>clns routing</td>
<td>Enable ISO connectionless routing on the switch.</td>
</tr>
<tr>
<td>Step 3</td>
<td></td>
</tr>
</tbody>
</table>
| router isis [area tag] | Enable the IS-IS routing for the specified routing process and enter IS-IS routing configuration mode.  
(Optional) Use the area tag argument to identify the area to which the IS-IS router is assigned. You must enter a value if you are configuring multiple IS-IS areas.  
The first IS-IS instance configured is Level 1-2 by default. Later instances are automatically Level 1. You can change the level of routing by using the is-type global configuration command. |

Table 36-12  Default IS-IS Configuration (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>No area or domain password is defined, and authentication is disabled.</td>
</tr>
<tr>
<td>Set-overload-bit</td>
<td>Disabled. When enabled, if no arguments are entered, the overload bit is set immediately and remains set until you enter the no set-overload-bit command.</td>
</tr>
</tbody>
</table>
| Shortest path first (SPF) throttling timers | Maximum interval between consecutive SFPs: 10 seconds.  
Initial SFP calculation after a topology change: 5500 ms.  
Holdtime between the first and second SFP calculation: 5500 ms. |
| Summary-address                  | Disabled.                                                                        |

1. NSF = Nonstop Forwarding
2. IS-IS NSF awareness is enabled for IPv4 on switches running Cisco IOS Release 12.2(25)SEG or later.
To disable IS-IS routing, use the `no router isis area-tag` router configuration command.

This example shows how to configure three routers to run conventional IS-IS as an IP routing protocol. In conventional IS-IS, all routers act as Level 1 and Level 2 routers (by default).

### Router A

```
Switch(config)# clns routing
Switch(config)# router isis
Switch(config-router)# net 49.0001.0000.0000.000a.00
Switch(config-router)# exit
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config-router)# exit
```

### Router B

```
Switch(config)# clns routing
Switch(config)# router isis
Switch(config-router)# net 49.0001.0000.0000.000b.00
Switch(config-router)# exit
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# ip router isis
```
Configuring IS-IS Global Parameters

These are some optional IS-IS global parameters that you can configure:

- You can force a default route into an IS-IS routing domain by configuring a default route controlled by a route map. You can also specify other filtering options configurable under a route map.
- You can configure the router to ignore IS-IS LSPs that are received with internal checksum errors or to purge corrupted LSPs, which causes the initiator of the LSP to regenerate it.
- You can assign passwords to areas and domains.
- You can create aggregate addresses that are represented in the routing table by a summary address (route-summarization). Routes learned from other routing protocols can also be summarized. The metric used to advertise the summary is the smallest metric of all the specific routes.
- You can set an overload bit.
- You can configure the LSP refresh interval and the maximum time that an LSP can remain in the router database without a refresh.
- You can set the throttling timers for LSP generation, shortest path first computation, and partial route computation.
- You can configure the switch to generate a log message when an IS-IS adjacency changes state (up or down).
- If a link in the network has a maximum transmission unit (MTU) size of less than 1500 bytes, you can lower the LSP MTU so that routing will still occur.
- The partition avoidance router configuration command prevents an area from becoming partitioned when full connectivity is lost among a Level1-2 border router, adjacent Level 1 routers, and end hosts.

Beginning in privileged EXEC mode, follow these steps to configure IS-IS parameters:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>clns routing</td>
</tr>
<tr>
<td></td>
<td>Enable ISO connectionless routing on the switch.</td>
</tr>
<tr>
<td>Step 3</td>
<td>router isis</td>
</tr>
<tr>
<td></td>
<td>Specify the IS-IS routing protocol and enter router configuration mode.</td>
</tr>
</tbody>
</table>
### Command Purpose

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4</td>
<td><code>default-information originate</code> &lt;br&gt; <code>[route-map map-name]</code></td>
<td>(Optional) Force a default route into the IS-IS routing domain. If you enter <code>route-map map-name</code>, the routing process generates the default route if the route map is satisfied.</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>ignore-lsp-errors</code></td>
<td>(Optional) Configure the router to ignore LSPs with internal checksum errors, instead of purging the LSPs. This command is enabled by default (corrupted LSPs are dropped). To purge the corrupted LSPs, enter the <code>no ignore-lsp-errors</code> router configuration command.</td>
</tr>
<tr>
<td>Step 6</td>
<td><code>area-password password</code></td>
<td>(Optional) Configure the area authentication password, which is inserted in Level 1 (station router level) LSPs.</td>
</tr>
<tr>
<td>Step 7</td>
<td><code>domain-password password</code></td>
<td>(Optional) Configure the routing domain authentication password, which is inserted in Level 2 (area router level) LSPs.</td>
</tr>
<tr>
<td>Step 8</td>
<td><code>summary-address address mask</code> &lt;br&gt; `[level-1</td>
<td>level-1-2</td>
</tr>
</tbody>
</table>
| Step 9 | `set-overload-bit [on-startup` <br> `{ seconds | wait-for-bgp}]` | (Optional) Set an overload bit (a hippity bit) to allow other routers to ignore the router in their shortest path first (SPF) calculations if the router is having problems.  
  - (Optional) `on-startup`—sets the overload bit only on startup. If `on-startup` is not specified, the overload bit is set immediately and remains set until you enter the `no set-overload-bit` command. If `on-startup` is specified, you must enter a number of seconds or `wait-for-bgp`.  
  - `seconds`—When the `on-startup` keyword is configured, causes the overload bit to be set upon system startup and remain set for this number of seconds. The range is from 5 to 86400 seconds.  
  - `wait-for-bgp`—When the `on-startup` keyword is configured, causes the overload bit to be set upon system startup and remain set until BGP has converged. If BGP does not signal IS-IS that it is converged, IS-IS will turn off the overload bit after 10 minutes. |
| Step 10| `lsp-refresh-interval seconds`               | (Optional) Set an LSP refresh interval in seconds. The range is from 1 to 65535 seconds. The default is to send LSP refreshes every 900 seconds (15 minutes). |
| Step 11| `max-lsp-lifetime seconds`                   | (Optional) Set the maximum time that LSP packets remain in the router database without being refreshed. The range is from 1 to 65535 seconds. The default is 1200 seconds (20 minutes). After the specified time interval, the LSP packet is deleted. |
| Step 12| `lsp-gen-interval [level-1 | level-2]` <br> `lsp-max-wait [lsp-initial-wait` <br> `lsp-second-wait]` | (Optional) Set the IS-IS LSP generation throttling timers:  
  - `lsp-max-wait`—the maximum interval (in seconds) between two consecutive occurrences of an LSP being generated. The range is 1 to 120, the default is 5.  
  - `lsp-initial-wait`—the initial LSP generation delay (in milliseconds). The range is 1 to 10000; the default is 50.  
  - `lsp-second-wait`—the hold time between the first and second LSP generation (in milliseconds). The range is 1 to 10000; the default is 5000. |
### Configuring ISO CLNS Routing

#### Command

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 13 | `spf-interval [level-1 | level-2]`
  `spf-max-wait [spf-initial-wait`
  `spf-second-wait]` | (Optional) Sets IS-IS shortest path first (SPF) throttling timers.  
  - `spf-max-wait`—the maximum interval between consecutive SFPs (in seconds). The range is 1 to 120; the default is 10.  
  - `spf-initial-wait`—the initial SFP calculation after a topology change (in milliseconds). The range is 1 to 10000; the default is 5500.  
  - `spf-second-wait`—the holdtime between the first and second SFP calculation (in milliseconds). The range is 1 to 10000; the default is 5500. |
| Step 14 | `prc-interval prc-max-wait`
  `[prc-initial-wait prc-second-wait]` | (Optional) Sets IS-IS partial route computation (PRC) throttling timers.  
  - `prc-max-wait`—the maximum interval (in seconds) between two consecutive PRC calculations. The range is 1 to 120; the default is 5.  
  - `prc-initial-wait`—the initial PRC calculation delay (in milliseconds) after a topology change. The range is 1 to 10,000; the default is 2000.  
  - `prc-second-wait`—the hold time between the first and second PRC calculation (in milliseconds). The range is 1 to 10,000; the default is 5000. |
| Step 15 | `log-adjacency-changes [all]` | (Optional) Set the router to log IS-IS adjacency state changes. Enter all to include all changes generated by events that are not related to the Intermediate System-to-Intermediate System Hellos, including End System-to-Intermediate System PDUs and link state packets (LSPs). |
| Step 16 | `lsp-mtu size` | (Optional) Specify the maximum LSP packet size in bytes. The range is 128 to 4352; the default is 1497 bytes.  
  **Note** If any link in the network has a reduced MTU size, you must change the LSP MTU size on all routers in the network. |
| Step 17 | `partition avoidance` | (Optional) Causes an IS-IS Level 1-2 border router to stop advertising the Level 1 area prefix into the Level 2 backbone when full connectivity is lost among the border router, all adjacent level 1 routers, and end hosts. |
| Step 18 | `end` | Return to privileged EXEC mode. |
| Step 19 | `show clns` | Verify your entries. |
| Step 20 | `copy running-config startup-config` | (Optional) Save your entries in the configuration file. |

To disable default route generation, use the `no default-information originate` router configuration command. Use the `no area-password` or `no domain-password` router configuration command to disable passwords. To disable LSP MTU settings, use the `no lsp mtu` router configuration command. To return to the default conditions for summary addressing, LSP refresh interval, LSP lifetime, LSP timers, SFP timers, and PRC timers, use the `no` form of the commands. Use the `no partition avoidance` router configuration command to disable the output format.

### Configuring IS-IS Interface Parameters

You can optionally configure certain interface-specific IS-IS parameters, independently from other attached routers. However, if you change some values from the defaults, such as multipliers and time intervals, it makes sense to also change them on multiple routers and interfaces. Most of the interface parameters can be configured for level 1, level 2, or both.
These are some interface level parameters you can configure:

- The default metric on the interface, which is used as a value for the IS-IS metric and assigned when there is no quality of service (QoS) routing performed.
- The hello interval (length of time between hello packets sent on the interface) or the default hello packet multiplier used on the interface to determine the hold time sent in IS-IS hello packets. The hold time determines how long a neighbor waits for another hello packet before declaring the neighbor down. This determines how quickly a failed link or neighbor is detected so that routes can be recalculated. Change the hello-multiplier in circumstances where hello packets are lost frequently and IS-IS adjacencies are failing unnecessarily. You can raise the hello multiplier and lower the hello interval correspondingly to make the hello protocol more reliable without increasing the time required to detect a link failure.
- Other time intervals:
  - Complete sequence number PDU (CSNP) interval. CSNPs are sent by the designated router to maintain database synchronization
  - Retransmission interval. This is the time between retransmission of IS-IS LSPs for point-to-point links.
  - IS-IS LSP retransmission throttle interval. This is the maximum rate (number of milliseconds between packets) at which IS-IS LSPs are re-sent on point-to-point links. This interval is different from the retransmission interval, which is the time between successive retransmissions of the same LSP
- Designated router election priority, which allows you to reduce the number of adjacencies required on a multiaccess network, which in turn reduces the amount of routing protocol traffic and the size of the topology database.
- The interface circuit type, which is the type of adjacency desired for neighbors on the specified interface
- Password authentication for the interface

Beginning in privileged EXEC mode, follow these steps to configure IS-IS interface parameters:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>interface interface-id</td>
<td>Specify the interface to be configured and enter interface configuration mode. If the interface is not already configured as a Layer 3 interface, enter the no switchport command to put it into Layer 3 mode.</td>
</tr>
<tr>
<td>3</td>
<td>isis metric default-metric [level-1</td>
<td>(Optional) Configure the metric (or cost) for the specified interface. The range is from 0 to 63. The default is 10. If no level is entered, the default is to apply to both Level 1 and Level 2 routers.</td>
</tr>
<tr>
<td></td>
<td>level-2]</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>isis hello-interval {seconds</td>
<td>(Optional) Specify the length of time between hello packets sent by the switch. By default, a value three times the hello interval seconds is advertised as the holdtime in the hello packets sent. With smaller hello intervals, topological changes are detected faster, but there is more routing traffic.</td>
</tr>
<tr>
<td></td>
<td>minimal} [level-1</td>
<td>minimal—causes the system to compute the hello interval based on the hello multiplier so that the resulting hold time is 1 second.</td>
</tr>
<tr>
<td></td>
<td>level-2]</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>seconds—the range is from 1 to 65535. The default is 10 seconds.</td>
</tr>
<tr>
<td>Command</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>isis hello-multiplier multiplier</strong> [level-1</td>
<td>level-2] (Optional) Specify the number of IS-IS hello packets a neighbor must miss before the router should declare the adjacency as down. The range is from 3 to 1000. The default is 3. Using a smaller hello-multiplier causes fast convergence, but can result in more routing instability.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>isis csnp-interval seconds</strong> [level-1</td>
<td>level-2] (Optional) Configure the IS-IS complete sequence number PDU (CSNP) interval for the interface. The range is from 0 to 65535. The default is 10 seconds.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>isis retransmit-interval seconds</strong> (Optional) Configure the number of seconds between retransmission of IS-IS LSPs for point-to-point links. The value you specify should be an integer greater than the expected round-trip delay between any two routers on the network. The range is from 0 to 65535. The default is 5 seconds.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><strong>isis retransmit-throttle-interval milliseconds</strong> (Optional) Configure the IS-IS LSP retransmission throttle interval, which is the maximum rate (number of milliseconds between packets) at which IS-IS LSPs will be re-sent on point-to-point links. The range is from 0 to 65535. The default is determined by the <strong>isis lsp-interval</strong> command.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td><strong>isis priority value</strong> [level-1</td>
<td>level-2] (Optional) Configure the priority to use for designated router election. The range is from 0 to 127. The default is 64.</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td><strong>isis circuit-type</strong> [level-1</td>
<td>level-1-2</td>
</tr>
<tr>
<td></td>
<td>• <strong>level-1</strong>—a Level 1 adjacency is established if there is at least one area address common to both this node and its neighbors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>level-1-2</strong>—a Level 1 and 2 adjacency is established if the neighbor is also configured as both Level 1 and Level 2 and there is at least one area in common. If there is no area in common, a Level 2 adjacency is established. This is the default.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>level 2</strong>—a Level 2 adjacency is established. If the neighbor router is a Level 1 router, no adjacency is established.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td><strong>isis password password</strong> [level-1</td>
<td>level-2] (Optional) Configure the authentication password for an interface. By default, authentication is disabled. Specifying Level 1 or Level 2 enables the password only for Level 1 or Level 2 routing, respectively. If you do not specify a level, the default is Level 1 and Level 2.</td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td><strong>end</strong> Return to privileged EXEC mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 13</strong></td>
<td><strong>show clns interface interface-id</strong> Verify your entries.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 14</strong></td>
<td><strong>copy running-config startup-config</strong> (Optional) Save your entries in the configuration file.</td>
<td></td>
</tr>
</tbody>
</table>

To return to the default settings, use the **no** forms of the commands.

## Monitoring and Maintaining ISO IGRP and IS-IS

You can remove all contents of a CLNS cache or remove information for a particular neighbor or route. You can display specific CLNS or IS-IS statistics, such as the contents of routing tables, caches, and databases. You can also display information about specific interfaces, filters, or neighbors.
Table 36-13 lists the privileged EXEC commands for clearing and displaying ISO CLNS and IS-IS routing. For explanations of the display fields, see the Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS and XNS Command Reference, Release 12.2, use the Cisco IOS command reference master index, or search online.

Table 36-13  ISO CLNS and IS-IS Clear and Show Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear clns cache</td>
<td>Clear and reinitialize the CLNS routing cache.</td>
</tr>
<tr>
<td>clear clns es-neighbors</td>
<td>Remove end system (ES) neighbor information from the adjacency database.</td>
</tr>
<tr>
<td>clear clns is-neighbors</td>
<td>Remove intermediate system (IS) neighbor information from the adjacency database.</td>
</tr>
<tr>
<td>clear clns neighbors</td>
<td>Remove CLNS neighbor information from the adjacency database.</td>
</tr>
<tr>
<td>clear clns route</td>
<td>Remove dynamically derived CLNS routing information.</td>
</tr>
<tr>
<td>show clns</td>
<td>Display information about the CLNS network.</td>
</tr>
<tr>
<td>show clns cache</td>
<td>Display the entries in the CLNS routing cache.</td>
</tr>
<tr>
<td>show clns es-neighbors</td>
<td>Display ES neighbor entries, including the associated areas.</td>
</tr>
<tr>
<td>show clns filter-expr</td>
<td>Display filter expressions.</td>
</tr>
<tr>
<td>show clns filter-set</td>
<td>Display filter sets.</td>
</tr>
<tr>
<td>show clns interface</td>
<td>Display the CLNS-specific or ES-IS information about each interface.</td>
</tr>
<tr>
<td>show clns neighbor</td>
<td>Display information about IS-IS neighbors.</td>
</tr>
<tr>
<td>show clns protocol</td>
<td>List the protocol-specific information for each IS-IS or ISO IGRP routing process in this router.</td>
</tr>
<tr>
<td>show clns route</td>
<td>Display all the destinations to which this router knows how to route CLNS packets.</td>
</tr>
<tr>
<td>show clns traffic</td>
<td>Display information about the CLNS packets this router has seen.</td>
</tr>
<tr>
<td>show ip route isis</td>
<td>Display the current state of the ISIS IP routing table.</td>
</tr>
<tr>
<td>show isis database</td>
<td>Display the IS-IS link-state database.</td>
</tr>
<tr>
<td>show isis routes</td>
<td>Display the IS-IS Level 1 routing table.</td>
</tr>
<tr>
<td>show isis spf-log</td>
<td>Display a history of the shortest path first (SPF) calculations for IS-IS.</td>
</tr>
<tr>
<td>show isis topology</td>
<td>Display a list of all connected routers in all areas.</td>
</tr>
<tr>
<td>show route-map</td>
<td>Display all route maps configured or only the one specified.</td>
</tr>
<tr>
<td>trace clns destination</td>
<td>Discover the paths taken to a specified destination by packets in the network.</td>
</tr>
<tr>
<td>which-route {nsap-address</td>
<td>clns-name}</td>
</tr>
</tbody>
</table>

Configuring BFD

The Bidirectional Forwarding Detection (BFD) Protocol quickly detects forwarding-path failures for a variety of media types, encapsulations, topologies, and routing protocols. It operates in a unicast, point-to-point mode on top of any data protocol being forwarded between two systems to track IPv4 connectivity between directly connected neighbors. BFD packets are encapsulated in UDP packets with a destination port number of 3784 or 3785.
In EIGRP, IS-IS, and OSPF deployments, the closest alternative to BFD is the use of modified failure-detection mechanisms. Although reducing the EIGRP, IS-IS, and OSPF timers can result in a failure-detection rate of 1 to 2 seconds, BFD can provide failure detection in less than 1 second. BFD can be less CPU-intensive than the reduced timers and, because it is not tied to any particular routing protocol, it can be used as a generic and consistent failure detection mechanism for multiple routing protocols.

To create a BFD session, you must configure BFD on both systems (BFD peers). Enabling BFD at the interface and routing protocol level on BFD peers creates a BFD session. BFD timers are negotiated and the BFD peers send control packets to each other at the negotiated intervals. If the neighbor is not directly connected, BFD neighbor registration is rejected.

Figure 36-6 shows a simple network with two routers running OSPF and BFD. When OSPF discovers a neighbor (1), it sends a request to the BFD process to initiate a BFD neighbor session with the neighbor OSPF router (2), establishing the BFD neighbor session (3).

Figure 36-6 Establishing a BFD Session

![Figure 36-6 Establishing a BFD Session](image)

Figure 36-7 shows what happens when a failure occurs in the network (1). The BFD neighbor session with the OSPF neighbor closes (2). BFD notifies the OSPF process that the BFD neighbor is no longer reachable, and the OSPF process breaks the OSPF neighbor relationship (4). If an alternative path is available, the routers start converging on it.

Figure 36-7 Breaking an OSPF Neighbor Relationship

![Figure 36-7 Breaking an OSPF Neighbor Relationship](image)

BFD clients are routing protocols that register neighbors with BFD. The switch supports ISIS, OSPF v1 and v2, BGP, EIGRP, and HSRP clients. You can use one BFD session for multiple client protocols. For example, if a network is running OSPF and EIGRP across the same link to the same peer, you need to create only one BFD session, and information is shared with both routing protocols.

The switch supports BFD version 0 and version 1. BFD neighbors automatically negotiate the version and the protocol always runs at the higher version. The default version is version 1.
By default, BFD neighbors exchange both control packets and echo packets for detecting forwarding failures. The switch sends echo packets at the configured BFD interval rate (from 50 to 999 ms on ports or from 600 to 999 ms on switch virtual interfaces), and control packets at the BFD slow-timer rate (from 1000 to 3000 ms).

Failure-rate detection can be faster in BFD echo mode, which is enabled by default when you configure BFD session. In this mode, the switch sends echo packets from the BFD software layer, and the BFD neighbor responds to the echo packets through its fast-switching layer. The echo packets do not reach the BFD neighbor software layer, but are reflected back over the forwarding path for failure detection. You configure the rate at which each BFD interface sends BFD echo packets by entering the `bfd interval` interface configuration command.

To reduce bandwidth consumption, you can disable the sending of echo packets by entering the `no bfd echo` interface configuration command. When BFD echo is disabled at one end of a link, the other end of the link also does not send echo packets and does not reflect back the echo packet. Control packets are used to detect forwarding failures. When BFD echo is disabled, the BFD slow-timer configuration does not apply. In a BFD session running in asynchronous mode, BFD packets are exchanged at a negotiated duration when the session is up and at the BFD slow-timer value when the session is down.

To run BFD on a switch, you need to configure basic BFD interval parameters on BFD interfaces, enable routing on the switch, and enable one or more one routing protocol clients for BFD. You also need to confirm that Cisco Express Forwarding (CEF) is enabled (the default) on participating switches.

For more detailed configuration, see the Bidirectional Forwarding Detection feature module at this URL: [http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fs_bfd.html](http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fs_bfd.html)

For details on the commands, use the Master Index to the Cisco IOS Command List for Release 12.4. at this URL:


These sections describe configuring BFD:

- Default BFD Configuration, page 36-75
- BFD Configuration Guidelines, page 36-76
- Configuring BFD Session Parameters on an Interface, page 36-77
- Enabling BFD Routing Protocol Clients, page 36-78

### Default BFD Configuration

No BFD sessions are configured. BFD is disabled on all interfaces.

When configured, BFD version 1 is the default, but switches negotiate for version. Version 0 is also supported.

Standby BFD (for HSRP) is enabled by default.

Asynchronous BFD echo mode is enabled when a BFD session is configured.
BFD Configuration Guidelines

- To run BFD on a switch:
  - Configure basic BFD interval parameters on each interface over which you want to run BFD sessions.
  - Enable routing on the switch. You can configure BFD without enabling routing, but BFD sessions do not become active unless routing is enabled on the switch and on the BFD interfaces.
  - Enable one or more one routing protocol clients for BFD. You should implement fast convergence for the routing protocol that you are using. See the IP routing documentation in this chapter or in the *Cisco IOS IP Configuration Guide, Release 12.2*, for information on configuring fast convergence.

**Note**

We recommend that you configure the BFD interval parameters on an interface before configuring the routing protocol commands, especially when using EIGRP.

- Confirm that CEF is enabled on participating switches (the default) as well as IP routing.
- BFD is supported on physical interfaces that are configured as routing interfaces. Starting with Cisco IOS release 12.2(55)SE, BFD is also supported on SVIs. As with physical interfaces, BFD sessions do not operate on an SVI until you put the SVI into Layer 3 mode by assigning it an IP address and enable routing on the switch.

**Note**

Entering the `bfd all-interfaces global configuration command` to enable BFD on all interfaces associated with a routing protocol enables BFD on all physical interfaces and SVIs associated with that routing protocol.

- The switch supports up to 28 BFD sessions at one time.
  - On BFD-enabled ports, the switch supports a minimum hello interval of 50 ms with a multiplier of 3. The multiplier specifies the minimum number of consecutive packets that can be missed before a session is declared down.
  - On BFD-enabled SVIs, the minimum hello interval is 600 ms with a multiplier of 3 or higher.
- BFD is not supported on SVIs or port channels.
- Although you can configure BFD interface commands on a Layer 2 port, BFD sessions do not operate on the interface unless it is configured as a Layer 3 interface (no switchport) and assigned an IP address.
- In HSRP BFD, standby BFD is enabled globally by default and on all interfaces. If you disable it on an interface, you then must disable and reenable it globally for BFD sessions to be active.
- When using BFD echo mode (the default), you should disable sending of ICMP redirect messages by entering the `no ip redirects` interface configuration command on the BFD interface.
Configuring BFD Session Parameters on an Interface

Before you can start a BFD session on an interface, you must put the interface into Layer 3 mode and set the baseline BFD parameters on it.

**Note**
Although you can configure BFD on Layer 2 interfaces, a BFD session cannot start until both interfaces are in Layer 3 mode and routing is enabled on the switch.

Beginning in privileged EXEC mode, follow these steps to configure BFD parameters on any interface participating in a BFD session:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
<td>Specify an interface for a BFD session, and enter interface configuration mode. Physical interfaces and SVIs support BFD.</td>
</tr>
<tr>
<td>Step 3</td>
<td>no switchport</td>
<td>Remove the interface from Layer 2 configuration mode (physical interfaces only).</td>
</tr>
<tr>
<td>Step 4</td>
<td>ip address ip-address subnet-mask</td>
<td>Configure the IP address and IP subnet mask.</td>
</tr>
<tr>
<td>Step 5</td>
<td>bfd interval milliseconds min_rx milliseconds multiplier value</td>
<td>Set BFD parameters for echo packets on the interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• interval—Specify the rate at which BFD echo packets are sent to BFD peers. The range is from 50 to 999 milliseconds (ms) on physical interfaces and from 600 to 999 ms on SVIs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• min_rx—Specify the rate at which BFD echo packets are expected to be received from BFD peers. The range is from 50 to 999 ms on physical interfaces and from 600 to 999 ms on SVIs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• multiplier—Specify the number of consecutive BFD echo packets that must be missed from a BFD peer before BFD declares that it is unavailable and informs the other BFD peer of the failure. The range is from 3 to 50.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note There are no baseline BFD parameter defaults.</td>
</tr>
<tr>
<td>Step 6</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 7</td>
<td>show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 8</td>
<td>show bfd neighbor detail</td>
<td>(Optional) Display the final configured or negotiated values when the session is created with a neighbor.</td>
</tr>
<tr>
<td>Step 9</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To remove the BFD parameter configuration, enter the `no bfd interval` interface configuration command.
Enabling BFD Routing Protocol Clients

After you configure BFD parameters on an interface, you can start a BFD session for one or more routing protocols. You must first enable routing by entering the `ip routing` global configuration command on the switch. Note that there can be more than one way to start a BFD session on an interface, depending on the routing protocol.

- Configuring BFD for OSPF, page 36-78
- Configuring BFD for IS-IS, page 36-79
- Configuring BFD for BGP, page 36-81
- Configuring BFD for EIGRP, page 36-81
- Configuring BFD for HSRP, page 36-82
- Disabling BFD Echo Mode, page 36-82

Configuring BFD for OSPF

When you start BFD sessions for OSPF, OSPF must be running on all participating devices. You can enable BFD support for OSPF by enabling it globally on all OSPF interfaces or by enabling it on one or more interfaces.

Configuring BFD for OSPF Globally

Beginning in privileged EXEC mode, follow these steps to configure OSPF BFD globally, and to optionally disable it on specific interfaces:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2: router ospf process-id</td>
<td>Specify an OSPF process, and enter router configuration mode.</td>
</tr>
<tr>
<td>Step 3: bfd all-interfaces</td>
<td>Enable BFD globally on all interfaces associated with the OSPF routing process.</td>
</tr>
<tr>
<td>Step 4: exit</td>
<td>(Optional) Return to global configuration mode if you want to disable BFD on one or more OSPF interfaces.</td>
</tr>
<tr>
<td>Step 5: interface interface-id</td>
<td>(Optional) Specify an interface, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 6: ip ospf bfd disable</td>
<td>(Optional) Disable BFD on the specified OSPF interface. Repeat Steps 5 and 6 for all OSPF interfaces on which you do not want to run BFD sessions.</td>
</tr>
<tr>
<td>Step 7: end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 8: show bfd neighbors [detail]</td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td>Step 9: copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable OSPF BFD on all interfaces, enter the `no bfd all-interfaces` router configuration command. To disable it on an interface, enter the `no ip ospf bfd` or the `ip ospf bfd disable` interface configuration command on the interface.

If you want to run OSPF BFD on only one or a few interfaces, you can enter the `ip ospf bfd` interface configuration command on those interfaces instead of enabling it globally. See the next procedure.
Chapter 36      Configuring IP Unicast Routing

Configuring BFD

If you try to configure OSPF BFD on a Layer 2 interface, the configuration is not recognized.

This is an example of configuring BFD for OSPF on all OSPF interfaces:

```
Switch(config)# router ospf 109
Switch(config-router)# bfd all-interfaces
Switch(config-router)# exit
```

Configuring BFD for OSPF on an Interface

Beginning in privileged EXEC mode, follow these steps to configure OSPF BFD on an individual interface:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 router ospf process-id</td>
<td>Specify an OSPF process, and enter router configuration mode.</td>
</tr>
<tr>
<td>Step 3 exit</td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td>Step 4 interface interface-id</td>
<td>(Specify an interface, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 5 ip ospf bfd</td>
<td>Enable BFD on the specified OSPF interface. Repeat Steps 3 and 4 for all OSPF interfaces on which you want to run BFD sessions.</td>
</tr>
<tr>
<td>Step 6 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 7 show bfd neighbors [detail]</td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td>Step 8 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable OSPF BFD on an interface, enter the `no ip ospf bfd` or the `ip ospf bfd disable` interface configuration command on the interface.

This is an example of configuring BFD for OSPF on a single interface:

```
Switch(config)# router ospf 109
Switch(config-router)# exit
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip ospf bfd
```

Configuring BFD for IS-IS

When you start BFD sessions for IS-IS, IS-IS must be running on all devices participating in BFD. You can enable BFD support for IS-IS by enabling it globally on all IS-IS interfaces or by enabling it on one or more interfaces.

Configuring BFD for IS-IS Globally

Beginning in privileged EXEC mode, follow these steps to configure IS-IS BFD globally, and to optionally disable it on specific interfaces:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 router is-is area-tag</td>
<td>Specify an IS-IS process and enter router configuration mode.</td>
</tr>
</tbody>
</table>

Command Purpose

Step 1 configure terminal Enter global configuration mode.
Step 2 router is-is area-tag Specify an IS-IS process and enter router configuration mode.
### Configuring BFD

**Command** | **Purpose**  
--- | ---  
**Step 3** | bfd all-interfaces  
To disable IS-IS BFD on all interfaces, enter the `no bfd all-interfaces` router configuration command.  
To disable it on the specified interface, enter the `no isis bfd` or the `isis bfd disable` interface configuration command on the interface.  

**Step 4** | exit  
(Optional) Return to global configuration mode if you want to disable BFD on one or more IS-IS interfaces.  

**Step 5** | interface interface-id  
(Optional) Specify an interface and enter interface configuration mode.  

**Step 6** | ip router isis  
(Optional) Enable IPv4 IS-IS routing on the interface.  

**Step 7** | isis bfd disable  
(Optional) Disable BFD on the IS-IS interface. Repeat Steps 5 through 7 for all IS-IS interfaces on which you do not want to run BFD sessions.  

**Step 8** | end  
Return to privileged EXEC mode.  

**Step 9** | show bfd neighbors [detail]  
Verify the configuration.  

**Step 10** | `copy running-config startup-config`  
(Optional) Save your entries in the configuration file.  

To disable IS-IS BFD on all interfaces, enter the `no bfd all-interfaces` router configuration command.  
To disable it on the specified interface, enter the `no isis bfd` or the `isis bfd disable` interface configuration command on the interface.  

**Note**  
Although IS-IS BFD operates only on Layer 3 interfaces, you can configure it on interfaces in Layer 2 or Layer 3 mode. When you enable it, you see this message:  
*ISIS BFD is reverting to router mode configuration, and remains disabled.*  

This is an example of setting fast convergence and configuring BFD for IS-IS on all IS-IS interfaces:  
```
Switch(config)# router isis tag1
Switch(config-router)# bfd all-interfaces
Switch(config-router)# exit
```

### Configuring BFD for IS-IS on an Interface

Beginning in privileged EXEC mode, follow these steps to configure IS-IS BFD on an individual interface:

**Command** | **Purpose**  
--- | ---  
**Step 1** | configure terminal  
Enter global configuration mode.  
**Step 2** | `router isis area-tag`  
Specify an IS-IS process and enter router configuration mode.  
**Step 3** | `exit`  
Return to global configuration mode.  
**Step 4** | interface interface-id  
(Specify an interface, and enter interface configuration mode.  
**Step 5** | `isis bfd`  
Enable BFD on the specified IS-IS interface. Repeat Steps 3 and 4 for all IS-IS interfaces on which you want to run BFD sessions.  
**Step 6** | `end`  
Return to privileged EXEC mode.  
**Step 7** | `show bfd neighbors [detail]`  
Verify the configuration.  
**Step 8** | `copy running-config startup-config`  
(Optional) Save your entries in the configuration file.
To disable IS-IS BFD on an interface, enter the `no isis bfd` or the `isis bfd disable` interface configuration command on the interface.

This is an example of configuring BFD for IS-IS on a single interface:

```
Switch(config)# router is-is tag1
Switch(config-router)# exit
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# isis bfd
```

### Configuring BFD for BGP

When you start BFD sessions for BGP, BGP must be running on all participating devices. You enter the IP address of the BFD neighbor to enable BFD for BGP.

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>router bgp as-tag</td>
</tr>
<tr>
<td>Step 3</td>
<td>neighbor ip-address fall-over bfd</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
</tr>
<tr>
<td>Step 5</td>
<td>show bfd neighbors [detail] &gt; show ip bgp neighbor</td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To disable BGP BFD, enter the `no neighbor ip-address fall-over bfd` router configuration command.

### Configuring BFD for EIGRP

When you start BFD sessions for EIGRP, EIGRP must be running on all participating devices. You can enable BFD support for EIGRP by globally enabling it on all EIGRP interfaces or by enabling it on one or more interfaces.

Beginning in privileged EXEC mode, follow these steps to configure EIGRP BFD:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>router eigrp as-number</td>
</tr>
<tr>
<td>Step 3</td>
<td>log-adjacency changes [detail]</td>
</tr>
</tbody>
</table>
| Step 4  | bfd {all-interfaces | interface interface-id} | Enable BFD for EIGRP.  
  - Enter **all-interfaces** to globally enable BFD on all interfaces associated with the EIGRP routing process  
  - Enter **interface interface-id** to enable BFD on a per-interface basis for one or more interfaces associated with the EIGRP routing process. |
To disable EIGRP BFD on all interfaces, enter the `no bfd all-interfaces` router configuration command. To disable it on an interface, enter the `no bfd interface interface-id` router configuration command.

**Configuring BFD for HSRP**

HSRP supports BFD by default; it is globally enabled on all interfaces. If HSRP support has been manually disabled, you can reenable it in interface or global configuration mode. All participating devices must have HSRP enabled and CEF enabled (the default).

Beginning in privileged EXEC mode, follow these steps to reenable HSRP BFD:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Specify an interface for a BFD session, and enter interface configuration mode. Only physical interfaces support BFD.</td>
</tr>
<tr>
<td>Step 3 ip address ip-address subnet-mask</td>
<td>Configure the IP address and IP subnet mask for the interface.</td>
</tr>
<tr>
<td>Step 4 standby [group-number] ip [ip-address] [secondary]</td>
<td>Activate HSRP.</td>
</tr>
<tr>
<td>Step 5 standby bfd</td>
<td>(Optional) Enable HSRP support for BFD on the interface.</td>
</tr>
<tr>
<td>Step 6 exit</td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td>Step 7 standby bfd all-interfaces</td>
<td>(Optional) Enable HSRP support for BFD on all interfaces.</td>
</tr>
<tr>
<td>Step 8 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 9 show standby neighbors</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 10 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable HSRP support for BFD on all interfaces, enter the `no standby bfd all-interfaces` global configuration command. To disable it on an interface, enter the `no standby bfd` interface configuration command.

**Note**

If you disable standby BFD on an interface by entering the `no standby bfd` interface configuration command, to activate BFD sessions on other interfaces, you must disable and reenable it globally by entering the `no standby bfd all-interfaces` global configuration command followed by the `standby bfd all-interfaces` global configuration command.

**Disabling BFD Echo Mode**

When you configure a BFD session, BFD echo mode is enabled by default on BFD interfaces. You can disable echo mode on an interface. When BFD echo is disabled at one end of a link, the other end of the link also does not send echo packets and does not reflect back the echo packet. Control packets are used...
to detect forwarding failures. When BFD echo is disabled, the BFD slow-timer configuration does not apply. In a BFD session running in asynchronous mode, BFD packets are exchanged at a negotiated duration when the session is up and at the BFD slow-timer value when the session is down.

Beginning in privileged EXEC mode, follow these steps to disable echo mode on a BFD interface:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>no bfd echo</td>
</tr>
<tr>
<td>Step 4</td>
<td>exit</td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
</tr>
<tr>
<td>Step 6</td>
<td>show bfd neighbors detail</td>
</tr>
<tr>
<td>Step 7</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To reenable echo mode on the interface, enter the bfd echo interface configuration command. To reenable echo mode on the switch, enter the bfd echo global configuration command.

## Configuring Multi-VRF CE

Virtual Private Networks (VPNs) provide a secure way for customers to share bandwidth over a service-provider backbone network. A VPN is a collection of sites sharing a common routing table. A customer site is connected to the service-provider network by one or more interfaces, and the service provider associates each interface with a VPN routing table, called a VPN routing/forwarding (VRF) table. In a multiprotocol label switching (MPLS) VPN deployment, all customers have their own customer-edge (CE) device, and every CE has a dedicated line connected to a provider-edge (PE) router.

With multiple VPN routing/forwarding (multi-VRF), multiple customers can share one CE, and only one physical link is needed between the CE and the PE. This is accomplished by extending some PE functionality to the shared CE devices. The shared CE maintains separate VRF tables for each customer and switches or routes packets for each customer based on the CE routing table. Multi-VRF CE allows a service provider to support two or more VPNs with overlapping IP addresses.

This section includes these topics:

- Understanding Multi-VRF CE, page 36-84
- Default Multi-VRF CE Configuration, page 36-86
- Multi-VRF CE Configuration Guidelines, page 36-86
- Configuring VRFs, page 36-88
- Configuring VRF-Aware Services, page 36-88
- Configuring Multicast VRFs, page 36-92
- Configuring a VPN Routing Session, page 36-92
- Configuring BGP PE to CE Routing Sessions, page 36-93
- Multi-VRF CE Configuration Example, page 36-94
- Displaying Multi-VRF CE Status, page 36-97
Understanding Multi-VRF CE

Multi-VRF CE is a feature that allows a service provider to support two or more VPNs, where IP addresses can be overlapped among the VPNs. Multi-VRF CE uses input interfaces to distinguish routes for different VPNs and forms virtual packet-forwarding tables by associating one or more Layer 3 interfaces with each VRF. Interfaces in a VRF can be either physical, such as Ethernet ports, or logical, such as VLAN SVIs, but an interface cannot belong to more than one VRF at any time.

**Note**

Multi-VRF CE interfaces must be Layer 3 interfaces.

Multi-VRF CE includes these devices:

- CE devices provide customers access to the service-provider network over a data link to one or more PE routers. The CE device advertises the site’s local routes to the router and learns the remote VPN routes from it. A Catalyst 3750 Metro switch can be a CE.

- PE routers exchange routing information with CE devices by using static routing or a routing protocol such as BGP, RIPv2, OSPF, IS-IS, or EIGRP. The PE is only required to maintain VPN routes for those VPNs to which it is directly attached, eliminating the need for the PE to maintain all of the service-provider VPN routes. Each PE router maintains a VRF for each of its directly connected sites. Multiple interfaces on a PE router can be associated with a single VRF if all of these sites participate in the same VPN. Each VPN is mapped to a specified VRF. After learning local VPN routes from CEs, a PE router exchanges VPN routing information with other PE routers by using internal BGP (IBPG). A Catalyst 3750 Metro switch would typically be used as a PE.

- Provider routers or core routers are any routers in the service-provider network that do not attach to CE devices.

With multi-VRF CE, multiple customers can share one CE, and only one physical link is used between the CE and the PE. The shared CE maintains separate VRF tables for each customer and switches or routes packets for each customer based on its own routing table. Multi-VRF CE extends limited PE functionality to a CE device, giving it the ability to maintain separate VRF tables to extend the privacy and security of a VPN to the branch office.

Figure 36-8 shows a configuration using Catalyst 3750 Metro switches as multiple virtual CEs. This scenario is suited for customers who have low bandwidth requirements for their VPN service, for example, small companies. In this case, multi-VRF CE support is required in the Catalyst 3750 Metro switches. Because multi-VRF CE is a Layer 3 feature, each interface in a VRF must be a Layer 3 interface.
When the CE switch receives a command to add a Layer 3 interface to a VRF, it sets up the appropriate mapping between the VLAN ID and the policy label in multi-VRF-CE-related data structures and adds the VLAN ID and policy label to the VLAN database.

When the multi-VRF CE is configured, the Layer 3 forwarding table is conceptually partitioned into two sections:

- The multi-VRF CE routing section contains the routes from different VPNs.
- The global routing section contains routes to non-VPN networks, such as the Internet.

VLAN IDs from different VRFs are mapped into different policy labels, which are used to distinguish the VRFs during processing. If no route is found in the multi-VRF CE section of the Layer 3 forwarding table, the global routing section is used to determine the forwarding path. For each new VPN route learned, the Layer 3 setup function retrieves the policy label by using the VLAN ID of the ingress port and inserts the policy label and new route to the multi-VRF CE routing section. If the packet is received from a routed port, the port internal VLAN ID number is used; if the packet is received from an SVI, the VLAN number is used.

This is the packet-forwarding process in a multi-VRF-CE-enabled network:

- When the switch receives a packet from a VPN, the switch looks up the routing table, based on the input policy label number. When a route is found, the switch forwards the packet to the PE.
- When the ingress PE receives a packet from the CE, it performs a VRF lookup. When a route is found, the router adds a corresponding MPLS label to the packet and sends it to the MPLS network.
- When an egress PE receives a packet from the network, it removes the label and uses the label to identify the correct VPN routing table. Then it performs the normal route lookup. When a route is found, it forwards the packet to the correct adjacency.
- When a CE receives a packet from an egress PE, it uses the input policy label to look up the correct VPN routing table. When a route is found, it forwards the packet within the VPN.

To configure VRF, you create a VRF table and specify the Layer 3 interface associated with the VRF. Then configure the routing protocols in the VPN and between the CE and the PE. BGP is the preferred routing protocol used to distribute VPN routing information across the provider’s backbone.

The multi-VRF CE network has three major components:

- VPN route target communities—lists of all other members of a VPN community. You need to configure VPN route targets for each VPN community member.

Figure 36-8 Catalyst 3750 Metro Switches Acting as Multiple Virtual CEs
Multiprotocol BGP peering of VPN community PE routers—propagates VRF reachability information to all members of a VPN community. You need to configure BGP peering in all PE routers within a VPN community.

VPN forwarding—transports all traffic between all VPN community members across a VPN service-provider network.

Default Multi-VRF CE Configuration

Table 36-14 shows the default VRF configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRF</td>
<td>Disabled. No VRFs are defined.</td>
</tr>
<tr>
<td>Maps</td>
<td>No import maps, export maps, or route maps are defined.</td>
</tr>
<tr>
<td>VRF maximum routes</td>
<td>8000 (total number of routes supported in hardware).</td>
</tr>
<tr>
<td>Forwarding table</td>
<td>The default for an interface is the global routing table.</td>
</tr>
</tbody>
</table>

Multi-VRF CE Configuration Guidelines

These are considerations when configuring VRF in your network:

- A switch with multi-VRF CE is shared by multiple customers, and each customer has its own routing table.
- Because customers use different VRF tables, the same IP addresses can be reused. Overlapped IP addresses are allowed in different VPNs.
- Multi-VRF CE lets multiple customers share the same physical link between the PE and the CE. Trunk ports with multiple VLANs separate packets among customers. Each customer has its own VLAN.
- Multi-VRF CE does not support all MPLS-VRF functionality. It does not support label exchange, LDP adjacency, or labeled packets.
- For the PE router, there is no difference between using multi-VRF CE or using multiple CEs. In Figure 36-8, multiple virtual Layer 3 interfaces are connected to the multi-VRF CE device.
- The switch supports configuring VRF by using physical ports, VLAN SVIs, or a combination of both. The SVIs can be connected through an access port or a trunk port.
- VRF and PBR are mutually exclusive on a switch interface. You cannot enable VRF when PBR is enabled on an interface. The reverse is also true; you cannot enable PBR on an interface when VRF is enabled on the interface.
- The switch supports a total of 26 VRFs and VPNs.
- A customer can use multiple VLANs as long as they do not overlap with those of other customers. A customer’s VLANs are mapped to a specific routing table ID that is used to identify the appropriate routing tables stored on the switch.
- A switch using VRF can support one global network and a total of 26 VRFs and VPNs.
- Most routing protocols (BGP, OSPF, IS-IS, RIP, and static routing) can be used between the CE and the PE. However, we recommend using external BGP (EBGP) for these reasons:
- BGP does not require multiple algorithms to communicate with multiple CEs.
- BGP is designed for passing routing information between systems run by different administrations.
- BGP makes it easy to pass attributes of the routes to the CE.

- Multi-VRF-CE does not support IGRP.
- Multi-VRF CE does not affect the packet switching rate.
- When multi-VRF CE is configured, you cannot assign the same Hot Standby Routing Protocol (HSRP) standby address to two different VPNs.
Configuring VRFs

Beginning in privileged EXEC mode, follow these steps to configure one or more VRFs. For complete syntax and usage information for the commands, see the switch command reference for this release and the Cisco IOS Switching Services Command Reference, Release 12.2.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip routing</td>
</tr>
<tr>
<td>Step 3</td>
<td>ip vrf vrf-name</td>
</tr>
<tr>
<td>Step 4</td>
<td>rd route-distinguisher</td>
</tr>
<tr>
<td>Step 5</td>
<td>route-target {export</td>
</tr>
<tr>
<td>Step 6</td>
<td>import map route-map</td>
</tr>
<tr>
<td>Step 7</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 8</td>
<td>ip vrf forwarding vrf-name</td>
</tr>
<tr>
<td>Step 9</td>
<td>end</td>
</tr>
<tr>
<td>Step 10</td>
<td>show ip vrf [brief</td>
</tr>
<tr>
<td>Step 11</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

Use the no ip vrf vrf-name global configuration command to delete a VRF and to remove all interfaces from it. Use the no ip vrf forwarding interface configuration command to remove an interface from the VRF.

Configuring VRF-Aware Services

IP services can be configured on global interfaces, and these services run within the global routing instance. IP services are enhanced to run on multiple routing instances; they are VRF-aware. Any configured VRF in the system can be specified for a VRF-aware service.

VRF-Aware services are implemented in platform-independent modules. VRF means multiple routing instances in Cisco IOS. Each platform has its own limit on the number of VRFs it supports.

VRF-aware services have the following characteristics:

- The user can ping a host in a user-specified VRF.
- ARP entries are learned in separate VRFs. The user can display Address Resolution Protocol (ARP) entries for specific VRFs.
These services are VRF-Aware:

- ARP
- Ping
- Simple Network Management Protocol (SNMP)
- Hot Standby Router Protocol (HSRP)
- Syslog
- Traceroute
- FTP and TFTP

**Note**

VRF-Aware services are not supported for Unicast Reverse Path Forwarding (uRPF).

**User Interface for ARP**

Beginning in privileged EXEC mode, follow these steps to configure VRF-aware services for ARP. For complete syntax and usage information for the commands, refer to the switch command reference for this release and the *Cisco IOS Switching Services Command Reference, Release 12.2*.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip arp vrf vrf-name</td>
<td>Display the ARP table in the specified VRF.</td>
</tr>
</tbody>
</table>

**User Interface for PING**

Beginning in privileged EXEC mode, follow these steps to configure VRF-aware services for ping. For complete syntax and usage information for the commands, refer to the switch command reference for this release and the *Cisco IOS Switching Services Command Reference, Release 12.2*.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>ping vrf vrf-name ip-host</td>
<td>Display the ARP table in the specified VRF.</td>
</tr>
</tbody>
</table>

**User Interface for SNMP**

Beginning in privileged EXEC mode, follow these steps to configure VRF-aware services for SNMP. For complete syntax and usage information for the commands, refer to the switch command reference for this release and the *Cisco IOS Switching Services Command Reference, Release 12.2*.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>snmp-server trap authentication vrf</td>
<td>Enable SNMP traps for packets on a VRF.</td>
</tr>
<tr>
<td>3</td>
<td>snmp-server engineID remote &lt;host&gt; vrf &lt;vyp instance&gt; &lt;engine-id string&gt;</td>
<td>Configure a name for the remote SNMP engine on a switch.</td>
</tr>
<tr>
<td>4</td>
<td>snmp-server host &lt;host&gt; vrf &lt;vyp instance&gt; traps &lt;community&gt;</td>
<td>Specify the recipient of an SNMP trap operation and specify the VRF table to be used for sending SNMP traps.</td>
</tr>
</tbody>
</table>
**User Interface for HSRP**

HSRP support for VRFs ensures that HSRP virtual IP addresses are added to the correct IP routing table. Beginning in privileged EXEC mode, follow these steps to configure VRF-aware services for HSRP. For complete syntax and usage information for the commands, refer to the switch command reference for this release and the *Cisco IOS Switching Services Command Reference, Release 12.2*.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>interface interface-id</code></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>no switchport</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>ip vrf forwarding &lt;vrf-name&gt;</code></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>ip address ip address</code></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>standby 1 ip ip address</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>end</td>
</tr>
</tbody>
</table>

**User Interface for Syslog**

Beginning in privileged EXEC mode, follow these steps to configure VRF-aware services for Syslog. For complete syntax and usage information for the commands, refer to the switch command reference for this release and the *Cisco IOS Switching Services Command Reference, Release 12.2*.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>logging on</code></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>logging host ip address vrf vrf name</code></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>logging buffered logging buffered size debugging</code></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>logging trap debugging</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>logging facility facility</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>end</td>
</tr>
</tbody>
</table>
**User Interface for Traceroute**

Beginning in privileged EXEC mode, follow these steps to configure VRF-aware services for traceroute. For complete syntax and usage information for the commands, refer to the switch command reference for this release and the *Cisco IOS Switching Services Command Reference, Release 12.2*.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>traceroute vrf vrf-name ipaddress</td>
<td>Specify the name of a VPN VRF in which to find the destination address.</td>
</tr>
</tbody>
</table>

**User Interface for FTP and TFTP**

So that FTP and TFTP are VRF-aware, you must configure some FTP/TFTP CLIs. For example, if you want to use a VRF table that is attached to an interface, say E1/0, you need to configure the CLI `ip [t]ftp source-interface E1/0` to inform [t]ftp to use a specific routing table. In this example, the VRF table is used to look up the destination IP address. These changes are backward-compatible and do not affect existing behavior. That is, you can use the source-interface CLI to send packets out a particular interface even if no VRF is configured on that interface.

To specify the source IP address for FTP connections, use the `ip ftp source-interface` show mode command. To use the address of the interface where the connection is made, use the `no` form of this command.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 ip ftp source-interface interface-type interface-number</td>
<td>Specify the source IP address for FTP connections.</td>
</tr>
<tr>
<td>Step 3 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

To specify the IP address of an interface as the source address for TFTP connections, use the `ip tftp source-interface` show mode command. To return to the default, use the `no` form of this command.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 ip tftp source-interface interface-type interface-number</td>
<td>Specify the source IP address for TFTP connections.</td>
</tr>
<tr>
<td>Step 3 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

**User Interface for VRF-Aware RADIUS**

To configure VRF-Aware RADIUS, you must first enable AAA on a RADIUS server. The switch supports the `ip vrf forwarding vrf-name` server-group configuration and the `ip radius source-interface` global configuration commands, as described in the Per VRF AAA Feature Guide at this URL: [http://www.cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ftvrfaaa.html](http://www.cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ftvrfaaa.html)
Configuring Multicast VRFs

Beginning in privileged EXEC mode, follow these steps to configure a multicast within a VRF table. For complete syntax and usage information for the commands, see the switch command reference for this release and the *Cisco IOS Switching Services Command Reference, Release 12.2*.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code> Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>ip routing</code> Enable IP routing mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>ip vrf vrf-name</code> Name the VRF, and enter VRF configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>rd route-distinguisher</code> Create a VRF table by specifying a route distinguisher. Enter either an AS number and an arbitrary number (xxx:y) or an IP address and an arbitrary number (A.B.C.D:y).</td>
</tr>
<tr>
<td>Step 5</td>
<td>`route-target {export</td>
</tr>
<tr>
<td>Step 6</td>
<td><code>import map route-map</code> (Optional) Associate a route map with the VRF.</td>
</tr>
<tr>
<td>Step 7</td>
<td><code>ip multicast-routing vrf vrf-name distributed</code> (Optional) Enable global multicast routing for VRF table.</td>
</tr>
<tr>
<td>Step 8</td>
<td><code>interface interface-id</code> Specify the Layer 3 interface to be associated with the VRF, and enter interface configuration mode. The interface can be a routed port or an SVI.</td>
</tr>
<tr>
<td>Step 9</td>
<td><code>ip vrf forwarding vrf-name</code> Associate the VRF with the Layer 3 interface.</td>
</tr>
<tr>
<td>Step 10</td>
<td><code>ip address ip-address mask</code> Configure IP address for the Layer 3 interface.</td>
</tr>
<tr>
<td>Step 11</td>
<td><code>ip pim sparse-dense mode</code> Enable PIM on the VRF-associated Layer 3 interface.</td>
</tr>
<tr>
<td>Step 12</td>
<td><code>end</code> Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 13</td>
<td>`show ip vrf [brief</td>
</tr>
<tr>
<td>Step 14</td>
<td><code>copy running-config startup-config</code> (Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

For more information about configuring a multicast within a Multi-VRF CE, see the *Cisco IOS IP Multicast Configuration Guide, Release 12.4*.

Configuring a VPN Routing Session

Routing within the VPN can be configured with any supported routing protocol (RIP, OSPF, IGRP, EIGRP, IS-IS or BGP) or with static routing. The configuration shown here is for OSPF, but the process is the same for other protocols.

**Note** To configure an EIGRP routing process to run within a VRF instance, you must configure an autonomous-system number by entering the `autonomous-system autonomous-system-number` address-family configuration mode command.
Beginning in privileged EXEC mode, follow these steps to configure OSPF in the VPN:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> router ospf process-id vrf vrf-name</td>
<td>Enable OSPF routing, specify a VPN forwarding table, and enter router configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong> log-adjacency-changes</td>
<td>(Optional) Log changes in the adjacency state. This is the default state.</td>
</tr>
<tr>
<td><strong>Step 4</strong> redistribute bgp</td>
<td>Set the switch to redistribute information from the BGP network to the OSPF network.</td>
</tr>
<tr>
<td>autonomous-system-number subnets</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> network network-number area area-id</td>
<td>Define a network address and mask on which OSPF runs and the area ID for that network address.</td>
</tr>
<tr>
<td><strong>Step 6</strong> end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 7</strong> show ip ospf process-id</td>
<td>Verify the configuration of the OSPF network.</td>
</tr>
<tr>
<td><strong>Step 8</strong> copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Use the **no router ospf process-id vrf vrf-name** global configuration command to disassociate the VPN forwarding table from the OSPF routing process.

### Configuring BGP PE to CE Routing Sessions

Beginning in privileged EXEC mode, follow these steps to configure a BGP PE to CE routing session:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> router bgp autonomous-system-number</td>
<td>Configure the BGP routing process with the AS number passed to other BGP routers, and enter router configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong> network network-number mask</td>
<td>Specify a network and mask to announce using BGP.</td>
</tr>
<tr>
<td>network-mask</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> redistribute ospf process-id match</td>
<td>Set the switch to redistribute OSPF internal routes.</td>
</tr>
<tr>
<td>internal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> network network-number area area-id</td>
<td>Define a network address and mask on which OSPF runs and the area ID for that network address.</td>
</tr>
<tr>
<td><strong>Step 6</strong> address-family ipv4 vrf vrf-name</td>
<td>Define BGP parameters for PE to CE routing sessions, and enter VRF address-family mode.</td>
</tr>
<tr>
<td><strong>Step 7</strong> neighbor address remote-as as-number</td>
<td>Define a BGP session between PE and CE routers.</td>
</tr>
<tr>
<td><strong>Step 8</strong> neighbor address activate</td>
<td>Activate the advertisement of the IPv4 address family.</td>
</tr>
<tr>
<td><strong>Step 9</strong> end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 10</strong> show ip bgp [ipv4] [neighbors]</td>
<td>Verify BGP configuration.</td>
</tr>
<tr>
<td><strong>Step 11</strong> copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Use the **no router bgp autonomous-system-number** global configuration command to delete the BGP routing process. Use the command with keywords to delete routing characteristics.
Multi-VRF CE Configuration Example

Figure 36-9 is a simplified example of the physical connections in a network similar to that in Figure 36-8. OSPF is the protocol used in VPN1, VPN2, and the global network. BGP is used in the CE-to-PE connections. The examples following the illustration show how to configure a Catalyst 3750 Metro switch as CE Switch A and the VRF configuration for customer switches D and F. Commands for configuring CE Switch C and the other customer switches are not included, but would be similar to those shown. The example also includes commands for configuring traffic to Switch A for a Catalyst 6000 or Catalyst 6500 switch acting as PE router.

Figure 36-9  Multi-VRF CE Configuration Example

Configuring Switch A

On Switch A, enable routing, and configure VRF.

Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip routing
Switch(config)# ip vrf v11
Switch(config-vrf)# rd 800:1
Switch(config-vrf)# route-target export 800:1
Switch(config-vrf)# route-target import 800:1
Switch(config-vrf)# exit
Switch(config)# ip vrf v12
Switch(config-vrf)# rd 800:2
Switch(config-vrf)# route-target export 800:2
Switch(config-vrf)# route-target import 800:2
Switch(config-vrf)# exit
Configure the loopback and physical interfaces on Switch A. Gigabit Ethernet port 1 is a trunk connection to the PE. Fast Ethernet ports 8 and 11 connect to VPNs:

Switch(config)# interface loopback1
Switch(config-if)# ip vrf forwarding v11
Switch(config-if)# ip address 8.8.1.8 255.255.255.0
Switch(config-if)# exit

Switch(config)# interface loopback2
Switch(config-if)# ip vrf forwarding v12
Switch(config-if)# ip address 8.8.2.8 255.255.255.0
Switch(config-if)# exit

Switch(config)# interface gigabitethernet1/1/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# no ip address
Switch(config-if)# exit

Switch(config)# interface fastethernet1/0/8
Switch(config-if)# switchport access vlan 208
Switch(config-if)# no ip address
Switch(config-if)# exit

Switch(config)# interface fastethernet1/0/11
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# no ip address
Switch(config-if)# exit

Configure the VLANs used on Switch A. VLAN 10 is used by VRF 11 between the CE and the PE. VLAN 20 is used by VRF 12 between the CE and the PE. VLANs 118 and 208 are used for VRF for the VPNs that include Switch F and Switch D, respectively:

Switch(config)# interface vlan10
Switch(config-if)# ip vrf forwarding v11
Switch(config-if)# ip address 38.0.0.8 255.255.255.0
Switch(config-if)# exit

Switch(config)# interface vlan20
Switch(config-if)# ip vrf forwarding v12
Switch(config-if)# ip address 83.0.0.8 255.255.255.0
Switch(config-if)# exit

Switch(config)# interface vlan118
Switch(config-if)# ip vrf forwarding v12
Switch(config-if)# ip address 118.0.0.8 255.255.255.0
Switch(config-if)# exit

Switch(config)# interface vlan208
Switch(config-if)# ip vrf forwarding v11
Switch(config-if)# ip address 208.0.0.8 255.255.255.0
Switch(config-if)# exit

Configure OSPF routing in VPN1 and VPN2.

Switch(config)# router ospf 1 vrf v11
Switch(config-router)# redistribute bgp 800 subnets
Switch(config-router)# network 208.0.0.0 0.0.0.255 area 0
Switch(config-router)# exit
Switch(config)# router ospf 2 vrf v12
Switch(config-router)# redistribute bgp 800 subnets
Switch(config-router)# network 118.0.0.0 0.0.0.255 area 0
Switch(config-router)# exit
Configure BGP for CE to PE routing.

```
Switch(config)# router bgp 800
Switch(config-router)# address-family ipv4 vrf vl2
Switch(config-router-af)# redistribute ospf 2 match internal
Switch(config-router-af)# neighbor 83.0.0.3 remote-as 100
Switch(config-router-af)# neighbor 83.0.0.3 activate
Switch(config-router-af)# network 8.8.2.0 mask 255.255.255.0
Switch(config-router-af)# exit

Switch(config-router)# address-family ipv4 vrf vl1
Switch(config-router-af)# redistribute ospf 1 match internal
Switch(config-router-af)# neighbor 38.0.0.3 remote-as 100
Switch(config-router-af)# neighbor 38.0.0.3 activate
Switch(config-router-af)# network 8.8.1.0 mask 255.255.255.0
Switch(config-router-af)# end
```

Configuring Switch D

Switch D belongs to VPN 1 and is connected to Switch A by using these commands.

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip routing
Switch(config)# interface fastethernet1/0/2
Switch(config-if)# no switchport
Switch(config-if)# ip address 208.0.0.20 255.255.255.0
Switch(config-if)# exit

Switch(config)# router ospf 101
Switch(config-router)# network 208.0.0.0 0.0.0.255 area 0
Switch(config-router)# end
```

Configuring Switch F

Switch F belongs to VPN 2 and is connected to Switch A by using these commands.

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip routing
Switch(config)# interface fastethernet1/0/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# no ip address
Switch(config-if)# exit

Switch(config)# interface Vlan118
Switch(config-if)# ip address 118.0.0.11 255.255.255.0
Switch(config-if)# exit

Switch(config)# router ospf 101
Switch(config-router)# network 118.0.0.0 0.0.0.255 area 0
Switch(config-router)# end
```

Configuring the PE Switch B

On Switch B (the PE router), these commands configure the connections to the CE device, Switch A.

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip vrf vl
Router(config-vrf)# rd 100:1
```
Displaying Multi-VRF CE Status

You can use the privileged EXEC commands in Table 36-6 to display information about multi-VRF CE configuration and status.

**Table 36-15**  Show IP OSPF Statistics Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip protocols vrf vrf-name</td>
<td>Display routing protocol information associated with a VRF.</td>
</tr>
</tbody>
</table>
Table 36-15  Show IP OSPF Statistics Commands (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip route vrf vrf-name [connected] [protocol [as-number]] [list] [mobile] [odr] [profile] [static] [summary] [supernets-only]</code></td>
<td>Display IP routing table information associated with a VRF.</td>
</tr>
<tr>
<td>`show ip vrf [brief</td>
<td>detail</td>
</tr>
</tbody>
</table>

For more information about the information in the displays, see the *Cisco IOS Switching Services Command Reference, Release 12.2.*

### Configuring Protocol-Independent Features

This section describes how to configure IP routing protocol-independent features. For a complete description of the IP routing protocol-independent commands in this chapter, see the “IP Routing Protocol-Independent Commands” chapter of the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2.*

This section includes these procedures:

- Configuring Cisco Express Forwarding, page 36-98
- Configuring the Number of Equal-Cost Routing Paths, page 36-99
- Configuring Static Unicast Routes, page 36-100
- Specifying Default Routes and Networks, page 36-101
- Using Route Maps to Redistribute Routing Information, page 36-102
- Configuring Policy-Based Routing, page 36-106
- Filtering Routing Information, page 36-109
- Managing Authentication Keys, page 36-111

### Configuring Cisco Express Forwarding

Cisco Express Forwarding (CEF) is a Layer 3 IP switching technology used to optimize network performance. CEF implements an advanced IP look-up and forwarding algorithm to deliver maximum Layer 3 switching performance. CEF is less CPU-intensive than fast switching route caching, allowing more CPU processing power to be dedicated to packet forwarding. In dynamic networks, fast switching cache entries are frequently invalidated because of routing changes, which can cause traffic to be process-switched using the routing table, instead of fast switched using the route cache. CEF uses the Forwarding Information Base (FIB) lookup table to perform destination-based switching of IP packets.

The two main components in CEF are the distributed FIB and the distributed adjacency tables.

- The FIB is similar to a routing table or information base and maintains a mirror image of the forwarding information in the IP routing table. When routing or topology changes occur in the network, the IP routing table is updated, and those changes are reflected in the FIB. The FIB maintains next-hop address information based on the information in the IP routing table. Because the FIB contains all known routes that exist in the routing table, CEF eliminates route cache maintenance, is more efficient for switching traffic, and is not affected by traffic patterns.
Nodes in the network are said to be adjacent if they can reach each other with a single hop across a link layer. CEF uses adjacency tables to prepend Layer 2 addressing information. The adjacency table maintains Layer 2 next-hop addresses for all FIB entries.

Because the Catalyst 3750 Metro switch uses Application Specific Integrated Circuits (ASICs) to achieve Gigabit-speed line rate IP traffic, CEF forwarding applies only to the software-forwarding path; that is, traffic that is forwarded by the CPU.

The default configuration, which we recommend, is CEF enabled on all Layer 3 interfaces. Entering the `no ip route-cache cef` interface configuration command disables CEF for traffic that is being forwarded by software. This command does not affect the hardware forwarding path. Disabling CEF and using the `debug ip packet detail` privileged EXEC command can be useful when you want to debug software-forwarded traffic. To enable CEF on an interface for the software-forwarding path, use the `ip route-cache cef` interface configuration command. If for some reason CEF is globally disabled, you can re-enable it by using the `ip cef` global configuration command.

**Caution**

Although the `no ip route-cache cef` interface configuration command to disable CEF on an interface is visible in the CLI, we strongly recommend that you do not disable CEF on interfaces except for debugging purposes.

Beginning in privileged EXEC mode, follow these steps to enable CEF globally and on an interface in case, if, for some reason, it has been disabled:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>config terminal</td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip cef</td>
</tr>
<tr>
<td></td>
<td>Enable CEF operation.</td>
</tr>
<tr>
<td>Step 3</td>
<td>interface interface-id</td>
</tr>
<tr>
<td></td>
<td>Enter interface configuration mode, and specify the Layer 3 interface to configure.</td>
</tr>
<tr>
<td>Step 4</td>
<td>ip route-cache cef</td>
</tr>
<tr>
<td></td>
<td>Enable CEF on the interface for software-forwarded traffic.</td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
</tr>
<tr>
<td></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 6</td>
<td>show ip cef</td>
</tr>
<tr>
<td></td>
<td>Display the CEF status on all interfaces.</td>
</tr>
<tr>
<td>Step 7</td>
<td>show cef interface [interface-id]</td>
</tr>
<tr>
<td></td>
<td>Display detailed CEF information for all interfaces or the specified interface.</td>
</tr>
<tr>
<td>Step 8</td>
<td>show adjacency</td>
</tr>
<tr>
<td></td>
<td>Display CEF adjacency table information.</td>
</tr>
<tr>
<td>Step 9</td>
<td>copy running-config startup-config</td>
</tr>
<tr>
<td></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

### Configuring the Number of Equal-Cost Routing Paths

When a router has two or more routes to the same network with the same metrics, these routes can be thought of as having an equal cost. The term *parallel path* is another way to refer to occurrences of equal-cost routes in a routing table. If a router has two or more equal-cost paths to a network, it can use them concurrently. Parallel paths provide redundancy in case of a circuit failure and also enable a router to load balance packets over the available paths for more efficient use of available bandwidth.

Although the router automatically learns about and configures equal-cost routes, you can control the maximum number of parallel paths supported by an IP routing protocol in its routing table.
Beginning in privileged EXEC mode, follow these steps to change the maximum number of parallel paths installed in a routing table from the default:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>router { bgp</td>
</tr>
<tr>
<td>Step 3</td>
<td>maximum-paths maximum</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
</tr>
<tr>
<td>Step 5</td>
<td>show ip protocols</td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

Use the no maximum-paths router configuration command to restore the default value.

### Configuring Static Unicast Routes

Static unicast routes are user-defined routes that cause packets moving between a source and a destination to take a specified path. Static routes can be important if the router cannot build a route to a particular destination and are useful for specifying a gateway of last resort to which all unroutable packets are sent.

Beginning in privileged EXEC mode, follow these steps to configure a static route:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip route prefix mask { address</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
</tr>
<tr>
<td>Step 4</td>
<td>show ip route</td>
</tr>
<tr>
<td>Step 5</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

Use the no ip route prefix mask { address | interface } global configuration command to remove a static route.
The switch retains static routes until you remove them. However, you can override static routes with dynamic routing information by assigning administrative distance values. Each dynamic routing protocol has a default administrative distance, as listed in Table 36-16. If you want a static route to be overridden by information from a dynamic routing protocol, set the administrative distance of the static route higher than that of the dynamic protocol.

**Table 36-16 Dynamic Routing Protocol Default Administrative Distances**

<table>
<thead>
<tr>
<th>Route Source</th>
<th>Default Distance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected interface</td>
<td>0</td>
</tr>
<tr>
<td>Static route</td>
<td>1</td>
</tr>
<tr>
<td>Enhanced IRGP summary route</td>
<td>5</td>
</tr>
<tr>
<td>External BGP</td>
<td>20</td>
</tr>
<tr>
<td>Internal Enhanced IGRP</td>
<td>90</td>
</tr>
<tr>
<td>IGRP</td>
<td>100</td>
</tr>
<tr>
<td>OSPF</td>
<td>110</td>
</tr>
<tr>
<td>RIP</td>
<td>120</td>
</tr>
<tr>
<td>Internal BGP</td>
<td>200</td>
</tr>
<tr>
<td>Unknown</td>
<td>225</td>
</tr>
</tbody>
</table>

Static routes that point to an interface are advertised through RIP, IGRP, and other dynamic routing protocols, whether or not static `redistribute` router configuration commands were specified for those routing protocols. These static routes are advertised because static routes that point to an interface are considered in the routing table to be connected and hence lose their static nature. However, if you define a static route to an interface that is not one of the networks defined in a network command, no dynamic routing protocols advertise the route unless a `redistribute` static command is specified for these protocols.

When an interface goes down, all static routes through that interface are removed from the IP routing table. When the software can no longer find a valid next hop for the address specified as the forwarding router's address in a static route, the static route is also removed from the IP routing table.

**Specifying Default Routes and Networks**

A router might not be able to determine the routes to all other networks. To provide complete routing capability, you can use some routers as smart routers and give the remaining routers default routes to the smart router. (Smart routers have routing table information for the entire internetwork.) These default routes can be dynamically learned or can be configured in the individual routers. Most dynamic interior routing protocols include a mechanism for causing a smart router to generate dynamic default information that is then forwarded to other routers.

If a router has a directly connected interface to the specified default network, the dynamic routing protocols running on that device generate a default route. In RIP, it advertises the pseudonetwork 0.0.0.0.

A router that is generating the default for a network also might need a default of its own. One way a router can generate its own default is to specify a static route to the network 0.0.0.0 through the appropriate device.
Beginning in privileged EXEC mode, follow these steps to define a static route to a network as the static default route:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 ip default-network network number</td>
<td>Specify a default network.</td>
</tr>
<tr>
<td>Step 3 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4 show ip route</td>
<td>Display the selected default route in the gateway of last resort display.</td>
</tr>
<tr>
<td>Step 5 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Use the `no ip default-network network number` global configuration command to remove the route.

When default information is passed through a dynamic routing protocol, no further configuration is required. The system periodically scans its routing table to choose the optimal default network as its default route. In IGRP networks, there might be several candidate networks for the system default. Cisco routers use administrative distance and metric information to determine the default route or the gateway of last resort.

If dynamic default information is not being passed to the system, candidates for the default route are specified with the `ip default-network` global configuration command. If this network appears in the routing table from any source, it is flagged as a possible choice for the default route. If the router has no interface on the default network, but does have a path to it, the network is considered as a possible candidate, and the gateway to the best default path becomes the gateway of last resort.

### Using Route Maps to Redistribute Routing Information

The switch can run multiple routing protocols simultaneously, and it can redistribute information from one routing protocol to another. Redistributing information from one routing protocol to another applies to all supported IP-based routing protocols.

You can also conditionally control the redistribution of routes between routing domains by defining enhanced packet filters or route maps between the two domains. The `match` and `set` route-map configuration commands define the condition portion of a route map. The `match` command specifies that a criterion must be matched. The `set` command specifies an action to be taken if the routing update meets the conditions defined by the match command. Although redistribution is a protocol-independent feature, some of the `match` and `set` route-map configuration commands are specific to a particular protocol.

One or more `match` commands and one or more `set` commands follow a `route-map` command. If there are no `match` commands, everything matches. If there are no `set` commands, nothing is done, other than the match. Therefore, you need at least one `match` or `set` command.

**Note**

A route map with no `set` route-map configuration commands is sent to the CPU, which causes high CPU utilization.
You can also identify route-map statements as **permit** or **deny**. If the statement is marked as a deny, the packets meeting the match criteria are sent back through the normal forwarding channels (destination-based routing). If the statement is marked as permit, set clauses are applied to packets meeting the match criteria. Packets that do not meet the match criteria are forwarded through the normal routing channel.

You can use the BGP route map **continue** clause to execute additional entries in a route map after an entry is executed with successful match and set clauses. You can use the **continue** clause to configure and organize more modular policy definitions so that specific policy configurations need not be repeated within the same route map. Beginning in Cisco IOS Release 12.2(37)SE, the switch supports the **continue** clause for outbound policies. For more information about using the route map **continue** clause, see the BGP Route-Map Continue Support for an Outbound Policy feature guide for Cisco IOS Release 12.4(4)T at this URL:


**Note** Although each of Steps 3 through 14 in the following section is optional, you must enter at least one **match** route-map configuration command and one **set** route-map configuration command.

Beginning in privileged EXEC mode, follow these steps to configure a route map for redistribution:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong> Enter global configuration mode.</td>
</tr>
</tbody>
</table>
| **Step 2** | **route-map map-tag [permit | deny] [sequence number]** Define any route maps used to control redistribution and enter route-map configuration mode.  
| | **map-tag**—A meaningful name for the route map. The **redistribute** router configuration command uses this name to reference this route map. Multiple route maps might share the same map tag name.  
| | (Optional) If **permit** is specified and the match criteria are met for this route map, the route is redistributed as controlled by the set actions. If **deny** is specified, the route is not redistributed.  
| | **sequence number** (Optional)—Number that indicates the position a new route map is to have in the list of route maps already configured with the same name. |
| **Step 3** | **match as-path path-list-number** Match a BGP AS path access list. |
| **Step 4** | **match community-list community-list-number [exact]** Match a BGP community list. |
| **Step 5** | **match ip address {access-list-number | access-list-name} [...access-list-number | ...access-list-name]** Match a standard access list by specifying the name or number. It can be an integer from 1 to 199. |
| **Step 6** | **match metric metric-value** Match the specified route metric. The **metric-value** can be an EIGRP five-part metric with a specified value from 0 to 4294967295. |
| **Step 7** | **match ip next-hop {access-list-number | access-list-name} [...access-list-number | ...access-list-name]** Match a next-hop router address passed by one of the access lists specified (numbered from 1 to 199). |
### Configuring Protocol-Independent Features

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td><code>match tag tag value [...tag-value]</code></td>
<td>Match the specified tag value in a list of one or more route tag values. Each can be an integer from 0 to 4294967295.</td>
</tr>
<tr>
<td>9</td>
<td><code>match interface type number [...type number]</code></td>
<td>Match the specified next hop route out one of the specified interfaces.</td>
</tr>
<tr>
<td>10</td>
<td>`match ip route-source {access-list-number</td>
<td>access-list-name} [...access-list-number</td>
</tr>
</tbody>
</table>
| 11   | `match route-type {local | internal | external [type-1 | type-2]}` | Match the specified route-type:  
  - **local**—Locally generated BGP routes.  
  - **internal**—OSPF intra-area and interarea routes or EIGRP internal routes.  
  - **external**—OSPF external routes (Type 1 or Type 2) or EIGRP external routes. |
| 12   | `set dampening halflife reuse suppress max-suppress-time` | Set BGP route dampening factors. |
| 13   | `set local-preference value` | Assign a value to a local BGP path. |
| 14   | `set origin {igp | egp as | incomplete}` | Set the BGP origin code. |
| 15   | `set as-path {tag | prepend as-path-string}` | Modify the BGP autonomous system path. |
| 16   | `set level {level-1 | level-2 | level-1-2 | stub-area | backbone}` | Set the level for routes that are advertised into the specified area of the routing domain. The **stub-area** and **backbone** are OSPF NSSA and backbone areas. |
| 17   | `set metric metric value` | Set the metric value to give the redistributed routes (for EIGRP only). The **metric value** is an integer from -294967295 to 294967295. |
| 18   | `set metric bandwidth delay reliability loading mtu` | Set the metric value to give the redistributed routes (for EIGRP only):  
  - **bandwidth**—Metric value or IGRP bandwidth of the route in kilobits per second in the range 0 to 4294967295  
  - **delay**—Route delay in tens of microseconds in the range 0 to 4294967295.  
  - **reliability**—Likelihood of successful packet transmission expressed as a number between 0 and 255, where 255 means 100 percent reliability and 0 means no reliability.  
  - **loading**—Effective bandwidth of the route expressed as a number from 0 to 255 (255 is 100 percent loading).  
  - **mtu**—Minimum maximum transmission unit (MTU) size of the route in bytes in the range 0 to 4294967295. |
| 19   | `set metric-type {type-1 | type-2}` | Set the OSPF external metric type for redistributed routes. |
To delete an entry, use the `no route-map map tag` global configuration command or the `no match` or `no set` route-map configuration commands.

You can distribute routes from one routing domain into another and control route distribution. Beginning in privileged EXEC mode, follow these steps to control route redistribution. Note that the keywords are the same as defined in the previous procedure.

### Command Purpose

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td><code>set metric-type internal</code></td>
<td>Set the multi-exit discriminator (MED) value on prefixes advertised to external BGP neighbor to match the IGP metric of the next hop.</td>
</tr>
<tr>
<td>21</td>
<td><code>set weight</code></td>
<td>Set the BGP weight for the routing table. The value can be from 1 to 65535.</td>
</tr>
<tr>
<td>22</td>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>23</td>
<td><code>show route-map</code></td>
<td>Display all route maps configured or only the one specified to verify configuration.</td>
</tr>
<tr>
<td>24</td>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable redistribution, use the `no` form of the commands.

The metrics of one routing protocol do not necessarily translate into the metrics of another. For example, the RIP metric is a hop count, and the IGRP metric is a combination of five qualities. In these situations, an artificial metric is assigned to the redistributed route. Uncontrolled exchanging of routing information between different routing protocols can create routing loops and seriously degrade network operation.
If you have not defined a default redistribution metric that replaces metric conversion, some automatic metric translations occur between routing protocols:

- RIP can automatically redistribute static routes. It assigns static routes a metric of 1 (directly connected).
- Any protocol can redistribute other routing protocols if a default mode is in effect.

**Configuring Policy-Based Routing**

You can use policy-based routing (PBR) to configure a defined policy for traffic flows. By using PBR, you can have more control over routing by reducing the reliance on routes derived from routing protocols. PBR can determine and implement routing policies that allow or deny paths based on:

- Identity of a particular end system
- Application
- Protocol

You can use PBR to provide equal-access and source-sensitive routing, routing based on interactive versus batch traffic, or routing based on dedicated links. For example, you could transfer stock records to a corporate office on a high-bandwidth, high-cost link for a short time while transmitting routine application data such as e-mail over a low-bandwidth, low-cost link.

With PBR, you classify traffic using access control lists (ACLs) and then make traffic go through a different path. PBR is applied to incoming packets. All packets received on an interface with PBR enabled are passed through route maps. Based on the criteria defined in the route maps, packets are forwarded (routed) to the appropriate next hop.

- If packets do not match any route map statements, all set clauses are applied.
- If a statement is marked as permit and the packets do not match any route-map statements, the packets are sent through the normal forwarding channels, and destination-based routing is performed.
- For PBR, route-map statements marked as deny are not supported.

For more information about configuring route maps, see the “Using Route Maps to Redistribute Routing Information” section on page 36-102.

You can use standard IP ACLs to specify match criteria for a source address or extended IP ACLs to specify match criteria based on an application, a protocol type, or an end station. The process proceeds through the route map until a match is found. If no match is found, normal destination-based routing occurs. There is an implicit deny at the end of the list of match statements.

If match clauses are satisfied, you can use a set clause to specify the IP addresses identifying the next hop router in the path.

**Note**

For details about PBR commands and keywords, see the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2*. For a list of PBR commands that are visible but not supported by the switch, see Appendix C, “Unsupported Commands in Cisco IOS Release 12.2(55)SE.”
PBR Configuration Guidelines

Before configuring PBR, you should be aware of this information:

- Multicast traffic is not policy-routed. PBR applies to only to unicast traffic.
- You can enable PBR on a routed port or an SVI.
- VRF and PBR are mutually exclusive on a switch interface. You cannot enable VRF when PBR is enabled on an interface. The reverse is also true; you cannot enable PBR on an interface when VRF is enabled on the interface.
- The switch does not support route-map deny statements for PBR.
- You can apply a policy route map to an EtherChannel port channel in Layer 3 mode, but you cannot apply a policy route map to a physical interface that is a member of the EtherChannel. If you try to do so, the command is rejected. When a policy route map is applied to a physical interface, that interface cannot become a member of an EtherChannel.
- You can define a maximum of 246 IP policy route-maps on the switch.
- You can define a maximum of 512 access control entries (ACEs) for PBR on the switch.
- When configuring match criteria in a route map, follow these guidelines:
  - Do not match ACLs that permit packets destined for a local address. PBR would forward these packets, which could cause ping or Telnet failure or route protocol flapping.
  - Do not match ACLs with deny ACEs. Packets that match a deny ACE are sent to the CPU, which could cause high CPU utilization.
- The number of TCAM entries used by PBR depends on the route map itself, the ACLs used, and the order of the ACLs and route-map entries.
- Policy-based routing based on packet length, IP precedence and TOS, set interface, set default next hop, or set default interface are not supported. Policy maps with no valid set actions or with set action set to Don’t Fragment are not supported.

Enabling PBR

By default, PBR is disabled on the switch. To enable PBR, you must create a route map that specifies the match criteria and the resulting action if all of the match clauses are met. Then, you must enable PBR for that route map on an interface. All packets arriving on the specified interface matching the match clauses are subject to PBR.

PBR can be fast-switched or implemented at speeds that do not slow down the switch. Fast-switched PBR supports most match and set commands. PBR must be enabled before you enable fast-switched PBR. Fast-switched PBR is disabled by default.

Packets that are generated by the switch, or local packets, are not normally policy-routed. When you globally enable local PBR on the switch, all packets that originate on the switch are subject to local PBR. Local PBR is disabled by default.
Beginning in privileged EXEC mode, follow these steps to configure PBR:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> route-map map-tag [permit] [sequence number]</td>
<td>Define any route maps used to control where packets are output, and enter route-map configuration mode.</td>
</tr>
<tr>
<td></td>
<td>- <em>map-tag</em>—A meaningful name for the route map. The ip policy route-map interface configuration command uses this name to reference the route map. Multiple route maps might share the same map tag name.</td>
</tr>
<tr>
<td></td>
<td>- <em>(Optional) If <em>permit</em> is specified and the match criteria are met for this route map, the route is policy-routed as controlled by the set actions.</em></td>
</tr>
<tr>
<td>Note</td>
<td>The route-map <em>deny</em> statement is not supported in PBR route maps to be applied to an interface.</td>
</tr>
<tr>
<td></td>
<td>- <em>sequence number</em> <em>(Optional)</em>— Number that shows the position of a new route map in the list of route maps already configured with the same name.</td>
</tr>
<tr>
<td><strong>Step 3</strong> match ip address {access-list-number</td>
<td>access-list-name} [...access-list-number</td>
</tr>
<tr>
<td></td>
<td>- Note— Do not enter an ACL with a deny ACE or an ACL that permits a packet destined for a local address.</td>
</tr>
<tr>
<td></td>
<td>If you do not specify a <em>match</em> command, the route map applies to all packets.</td>
</tr>
<tr>
<td><strong>Step 4</strong> set ip next-hop ip-address [...]ip-address]</td>
<td>Specify the action to take on the packets that match the criteria. Set next hop to which to route the packet (the next hop must be adjacent).</td>
</tr>
<tr>
<td><strong>Step 5</strong> exit</td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 6</strong> interface interface-id</td>
<td>Enter interface configuration mode, and specify the interface to configure.</td>
</tr>
<tr>
<td><strong>Step 7</strong> ip policy route-map map-tag</td>
<td>Enable PBR on a Layer 3 interface, and identify the route map to use. You can configure only one route map on an interface. However, you can have multiple route map entries with different sequence numbers. These entries are evaluated in sequence number order until the first match. If there is no match, packets are routed as usual.</td>
</tr>
<tr>
<td><strong>Step 8</strong> ip route-cache policy</td>
<td><em>(Optional) Enable fast-switching PBR. You must first enable PBR before enabling fast-switching PBR.</em></td>
</tr>
<tr>
<td><strong>Step 9</strong> exit</td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 10</strong> ip local policy route-map map-tag</td>
<td><em>(Optional) Enable local PBR to perform policy-based routing on packets originating at the switch. This applies to packets generated by the switch and not to incoming packets.</em></td>
</tr>
<tr>
<td></td>
<td>- <em>Note</em>— If the IP policy route map contains a <em>deny</em> statement, the configuration fails.</td>
</tr>
<tr>
<td><strong>Step 11</strong> end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
## Filtering Routing Information

You can filter routing protocol information by performing the tasks described in this section.

**Note**

When routes are redistributed between OSPF processes, no OSPF metrics are preserved.

### Setting Passive Interfaces

To prevent other routers on a local network from dynamically learning about routes, you can use the `passive-interface` router configuration command to keep routing update messages from being sent through a router interface. When you use this command in the OSPF protocol, the interface address you specify as passive appears as a stub network in the OSPF domain. OSPF routing information is neither sent nor received through the specified router interface.

In networks with many interfaces, to avoid having to manually set them as passive, you can set all interfaces to be passive by default by using the `passive-interface default` router configuration command and manually setting interfaces where adjacencies are desired.

Beginning in privileged EXEC mode, follow these steps to configure passive interfaces:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>`router { bgp</td>
</tr>
<tr>
<td>`router { bgp</td>
<td>eigrp</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>passive-interface interface-id</code></td>
</tr>
<tr>
<td><code>passive-interface interface-id</code></td>
<td>Suppress sending routing updates through the specified Layer 3 interface.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>passive-interface default</code></td>
</tr>
<tr>
<td><code>passive-interface default</code></td>
<td>(Optional) Set all interfaces as passive by default.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>no passive-interface interface type</code></td>
</tr>
<tr>
<td><code>no passive-interface interface type</code></td>
<td>(Optional) Activate only those interfaces that need to have adjacencies sent.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>network network-address</code></td>
</tr>
<tr>
<td><code>network network-address</code></td>
<td>(Optional) Specify the list of networks for the routing process. The network-address is an IP address.</td>
</tr>
</tbody>
</table>
Use a network monitoring privileged EXEC command such as `show ip ospf interface` to verify the interfaces that you enabled as passive, or use the `show ip interface` privileged EXEC command to verify the interfaces that you enabled as active.

To re-enable the sending of routing updates, use the `no passive-interface interface-id` router configuration command. The `default` keyword sets all interfaces as passive by default. You can then configure individual interfaces where you want adjacencies by using the `no passive-interface` router configuration command. The `default` keyword is useful in Internet service provider and large enterprise networks where many of the distribution routers have more than 200 interfaces.

### Controlling Advertising and Processing in Routing Updates

You can use the `distribute-list` router configuration command with access control lists to suppress routes from being advertised in routing updates and to prevent other routers from learning one or more routes. When used in OSPF, this feature applies to only external routes, and you cannot specify an interface name.

You can also use a `distribute-list` router configuration command to avoid processing certain routes listed in incoming updates. (This feature does not apply to OSPF.)

Beginning in privileged EXEC mode, follow these steps to control the advertising or processing of routing updates:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>router { bgp</td>
</tr>
<tr>
<td>Step 3</td>
<td>distribute-list { access-list-number</td>
</tr>
<tr>
<td>Step 4</td>
<td>distribute-list { access-list-number</td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

Use the `no distribute-list in` router configuration command to change or cancel a filter. To cancel suppression of network advertisements in updates, use the `no distribute-list out` router configuration command.

### Filtering Sources of Routing Information

Because some routing information might be more accurate than others, you can use filtering to prioritize information coming from different sources. An *administrative distance* is a rating of the trustworthiness of a routing information source, such as a router or group of routers. In a large network, some routing protocols can be more reliable than others. By specifying administrative distance values, you enable the
router to intelligently discriminate between sources of routing information. The router always picks the route whose routing protocol has the lowest administrative distance. Table 36-16 on page 36-101 shows the default administrative distances for various routing information sources.

Because each network has its own requirements, there are no general guidelines for assigning administrative distances.

Beginning in privileged EXEC mode, follow these steps to filter sources of routing information:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>configure terminal</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
</tbody>
</table>

| Step 2 | router {bgp | eigrp | isis | iso-igrp | ospf | rip} | Enter router configuration mode. |
|--------|-------------------|---------|

<table>
<thead>
<tr>
<th>Step 3</th>
<th>distance weight {ip-address {ip-address mask}} [ip access list]</th>
<th>Define an administrative distance.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>weight—The administrative distance as an integer from 10 to 255. Used alone, weight specifies a default administrative distance that is used when no other specification exists for a routing information source. Routes with a distance of 255 are not installed in the routing table. (Optional) ip access list—An IP standard or extended access list to be applied to incoming routing updates.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>end</th>
<th>Return to privileged EXEC mode.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>show ip protocols</th>
<th>Display the default administrative distance for a specified routing process.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>copy running-config startup-config</th>
<th>(Optional) Save your entries in the configuration file.</th>
</tr>
</thead>
</table>

To remove a distance definition, use the no distance router configuration command.

### Managing Authentication Keys

Key management is a method of controlling authentication keys used by routing protocols. Not all protocols can use key management. Authentication keys are available for EIGRP and RIP Version 2.

Before you manage authentication keys, you must enable authentication. See the appropriate protocol section to see how to enable authentication for that protocol. To manage authentication keys, define a key chain, identify the keys that belong to the key chain, and specify how long each key is valid. Each key has its own key identifier (specified with the key number key chain configuration command), which is stored locally. The combination of the key identifier and the interface associated with the message uniquely identifies the authentication algorithm and Message Digest 5 (MD5) authentication key in use.

You can configure multiple keys with lifetimes. Only one authentication packet is sent, regardless of how many valid keys exist. The software examines the key numbers in order from lowest to highest, and uses the first valid key it encounters. The lifetimes allow for overlap during key changes. Note that the router must know these lifetimes.

Beginning in privileged EXEC mode, follow these steps to manage authentication keys:
To remove the key chain, use the `no key chain name-of-chain` global configuration command.

### Monitoring and Maintaining the IP Network

You can remove all contents of a particular cache, table, or database. You can also display specific statistics. Use the privileged EXEC commands in Table 36-17 to clear routes or display status:

**Table 36-17 Commands to Clear IP Routes or Display Route Status**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip route `{network [mask</td>
<td>*]}`</td>
</tr>
<tr>
<td>show ip protocols</td>
<td>Display the parameters and state of the active routing protocol process.</td>
</tr>
<tr>
<td>show ip route `{address [mask] [longer-pREFIXES]]</td>
<td>(protocol [process-id])`</td>
</tr>
<tr>
<td>show ip route summary</td>
<td>Display the current state of the routing table in summary form.</td>
</tr>
<tr>
<td>show ip route supernets-only</td>
<td>Display supernets.</td>
</tr>
</tbody>
</table>
### Table 36-17  Commands to Clear IP Routes or Display Route Status (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip cache</code></td>
<td>Display the routing table used to switch IP traffic.</td>
</tr>
<tr>
<td><code>show route-map [map-name]</code></td>
<td>Display all route maps configured or only the one specified.</td>
</tr>
</tbody>
</table>
CHAPTER 37

Configuring IPv6 Unicast Routing

This chapter describes how to configure IPv6 unicast routing on the Catalyst 3750 Metro switch.

For information about configuring IPv6 Multicast Listener Discovery (MLD) snooping, see Chapter 38, “Configuring IPv6 MLD Snooping.” For information on configuring IPv6 access control lists (ACLs), see Chapter 39, “Configuring IPv6 ACLs.” For information about configuring IPv4 unicast routing, see Chapter 36, “Configuring IP Unicast Routing.”

To enable IPv6 routing, you must configure the switch to use the a dual IPv4 and IPv6 switch database management (SDM) template. See the “Dual IPv4 and IPv6 Protocol Stacks” section on page 37-5.

For complete syntax and usage information for the commands used in this chapter, see the Cisco IOS IPv6 Command Reference:

This chapter consists of these sections:

- “Understanding IPv6” section on page 37-1
- “Configuring IPv6” section on page 37-9
- “Displaying IPv6” section on page 37-24

Understanding IPv6

IPv4 users can move to IPv6 and receive services such as end-to-end security, quality of service (QoS), and globally unique addresses. The IPv6 address space reduces the need for private addresses and Network Address Translation (NAT) processing by border routers at network edges.

For information about IPv6 and other features in this chapter

- See the Cisco IOS IPv6 Configuration Guide:
- Use the Search field to locate the Cisco IOS software documentation. For example, if you want information about static routes, you can enter Implementing Static Routes for IPv6 in the search field to get this document about static routes:
This section describes IPv6 implementation on the switch. These sections are included:

- IPv6 Addresses, page 37-2
- Supported IPv6 Unicast Routing Features, page 37-2
- Unsupported IPv6 Unicast Routing Features, page 37-8
- Limitations, page 37-8

## IPv6 Addresses

The switch supports only IPv6 unicast addresses. It does not support site-local unicast addresses, anycast addresses, or multicast addresses.

The IPv6 128-bit addresses are represented as a series of eight 16-bit hexadecimal fields separated by colons in the format: n:n:n:n:n:n:n:n. This is an example of an IPv6 address:

\[2031:0000:130F:0000:0000:09C0:080F:130B\]

For easier implementation, leading zeros in each field are optional. This is the same address without leading zeros:

\[2031:0:130F:0:0:9C0:80F:130B\]

You can also use two colons (::) to represent successive hexadecimal fields of zeros, but you can use this short version only once in each address:

\[2031:0:130F::09C0:080F:130B\]

For more information about IPv6 address formats, address types, and the IPv6 packet header, see the “Implementing IPv6 Addressing and Basic Connectivity” chapter of *Cisco IOS IPv6 Configuration Guide* on Cisco.com.

In the “Implementing Addressing and Basic Connectivity” chapter, these sections apply to the switch:

- IPv6 Address Formats
- IPv6 Address Type: Unicast
- IPv6 Address Output Display
- Simplified IPv6 Packet Header

## Supported IPv6 Unicast Routing Features

These sections describe the IPv6 protocol features supported by the switch:

- 128-Bit Wide Unicast Addresses, page 37-3
- DNS for IPv6, page 37-3
- Path MTU Discovery for IPv6 Unicast, page 37-4
- ICMPv6, page 37-4
- Neighbor Discovery, page 37-4
- Default Router Preference, page 37-4
- IPv6 Stateless Autoconfiguration and Duplicate Address Detection, page 37-4
- IPv6 Applications, page 37-5
- Dual IPv4 and IPv6 Protocol Stacks, page 37-5
• DHCP for IPv6 Address Assignment, page 37-6
• Static Routes for IPv6, page 37-6
• RIP for IPv6, page 37-6
• OSPF for IPv6, page 37-6
• EIGRP for IPv6, page 37-6
• Multiprotocol BGP for IPv6, page 37-7
• SNMP and Syslog Over IPv6, page 37-7
• HTTP(S) Over IPv6, page 37-7

Support on the switch includes expanded address capability, header format simplification, improved support of extensions and options, and hardware parsing of the extension header. The switch supports hop-by-hop extension header packets, which are routed or bridged in software.

The switch provides IPv6 routing capability over native Ethernet Inter-Switch Link (ISL) or 802.1Q trunk ports for static routes, Routing Information Protocol (RIP) for IPv6, and Open Shortest Path First (OSPF) Version 3 Protocol. It supports up to 16 equal-cost routes and can simultaneously forward IPv4 and IPv6 frames at line rate.

128-Bit Wide Unicast Addresses

The switch supports aggregatable global unicast addresses and link-local unicast addresses. It does not support site-local unicast addresses.

• Aggregatable global unicast addresses are IPv6 addresses from the aggregatable global unicast prefix. The address structure enables strict aggregation of routing prefixes and limits the number of routing table entries in the global routing table. These addresses are used on links that are aggregated through organizations and eventually to the Internet service provider.

These addresses are defined by a global routing prefix, a subnet ID, and an interface ID. Current global unicast address allocation uses the range of addresses that start with binary value 001 (2000::/3). Addresses with a prefix of 2000::/3(001) through E000::/3(111) must have 64-bit interface identifiers in the extended unique identifier (EUI)-64 format.

• Link local unicast addresses can be automatically configured on any interface by using the link-local prefix FE80::/10(1111 1110 10) and the interface identifier in the modified EUI format. Link-local addresses are used in the neighbor discovery protocol (NDP) and the stateless autoconfiguration process. Nodes on a local link use link-local addresses and do not require globally unique addresses to communicate. IPv6 routers do not forward packets with link-local source or destination addresses to other links.

For more information, see the section about IPv6 unicast addresses in the “Implementing IPv6 Addressing and Basic Connectivity” chapter in the Cisco IOS IPv6 Configuration Guide on Cisco.com.

DNS for IPv6

IPv6 supports Domain Name System (DNS) record types in the DNS name-to-address and address-to-name lookup processes. The DNS AAAA resource record types support IPv6 addresses and are equivalent to an A address record in IPv4. The switch supports DNS resolution for IPv4 and IPv6.
Path MTU Discovery for IPv6 Unicast

The switch supports advertising the system maximum transmission unit (MTU) to IPv6 nodes and path MTU discovery. Path MTU discovery allows a host to dynamically discover and adjust to differences in the MTU size of every link along a given data path. In IPv6, if a link along the path is not large enough to accommodate the packet size, the source of the packet handles the fragmentation. The switch does not support path MTU discovery for multicast packets.

ICMPv6

The Internet Control Message Protocol (ICMP) in IPv6 generates error messages, such as ICMP destination unreachable messages, to report errors during processing and other diagnostic functions. In IPv6, ICMP packets are also used in the neighbor discovery protocol and path MTU discovery.

Neighbor Discovery

The switch supports NDP for IPv6, a protocol running on top of ICMPv6, and static neighbor entries for IPv6 stations that do not support NDP. The IPv6 neighbor discovery process uses ICMP messages and solicited-node multicast addresses to determine the link-layer address of a neighbor on the same network (local link), to verify the reachability of the neighbor, and to keep track of neighboring routers.

The switch supports ICMPv6 redirect for routes with mask lengths less than 64 bits. ICMP redirect is not supported for host routes or for summarized routes with mask lengths greater than 64 bits.

Neighbor discovery throttling ensures that the switch CPU is not unnecessarily burdened while it is in the process of obtaining the next hop forwarding information to route an IPv6 packet. The switch drops any additional IPv6 packets whose next hop is the same neighbor that the switch is actively trying to resolve. This drop avoids further load on the CPU.

Default Router Preference

The switch supports IPv6 default router preference (DRP), an extension in router advertisement messages. DRP improves the ability of a host to select an appropriate router, especially when the host is multihomed and the routers are on different links. The switch does not support the Route Information Option in RFC 4191.

An IPv6 host maintains a default router list from which it selects a router for traffic to offlink destinations. The selected router for a destination is then cached in the destination cache. NDP for IPv6 specifies that routers that are reachable or probably reachable are preferred over routers whose reachability is unknown or suspect. For reachable or probably reachable routers, NDP can either select the same router every time or cycle through the router list. By using DRP, you can configure an IPv6 host to prefer one router over another, provided both are reachable or probably reachable.

For more information about DRP for IPv6, see the “Implementing IPv6 Addresses and Basic Connectivity” chapter in the Cisco IOS IPv6 Configuration Guide on Cisco.com.

IPv6 Stateless Autoconfiguration and Duplicate Address Detection

The switch uses stateless autoconfiguration to manage link, subnet, and site addressing changes, such as management of host and mobile IP addresses. A host autonomously configures its own link-local address, and booting nodes send router solicitations to request router advertisements for configuring interfaces.
For more information about autoconfiguration and duplicate address detection, see the “Implementing IPv6 Addressing and Basic Connectivity” chapter of *Cisco IOS IPv6 Configuration Guide* on Cisco.com.

**IPv6 Applications**

The switch has IPv6 support for these applications:
- Ping, traceroute, Telnet, TFTP, and FTP
- Secure Shell (SSH) over an IPv6 transport
- HTTP server access over IPv6 transport
- DNS resolver for AAAA over IPv4 transport
- Cisco Discovery Protocol (CDP) support for IPv6 addresses

For more information about managing these applications, see the “Managing Cisco IOS Applications over IPv6” chapter and the “Implementing IPv6 Addressing and Basic Connectivity” chapter in the *Cisco IOS IPv6 Configuration Guide* on Cisco.com.

**Dual IPv4 and IPv6 Protocol Stacks**

You must use the dual IPv4 and IPv6 template to allocate ternary content addressable memory (TCAM) usage to both IPv4 and IPv6 protocols.

Figure 37-1 shows a router forwarding both IPv4 and IPv6 traffic through the same interface, based on the IP packet and destination addresses.

*Figure 37-1     Dual IPv4 and IPv6 Support on an Interface*

Use the dual IPv4 and IPv6 SDM template to enable IPv6 routing. For more information about the dual IPv4 and IPv6 SDM template, see Chapter 6, “Configuring SDM Templates.”

The dual IPv4 and IPv6 templates allow the switch to be used in dual stack environments.
- If you try to configure IPv6 without first selecting a dual IPv4 and IPv6 template, a warning message appears.
- In IPv4-only environments, the switch routes IPv4 packets and applies IPv4 QoS and ACLs in hardware. IPv6 packets are not supported.
- In dual IPv4 and IPv6 environments, the switch routes both IPv4 and IPv6 packets and applies IPv4 QoS in hardware.
- Full IPv6 QoS is not supported.
If you do not plan to use IPv6, do not use the dual stack template because this template results in less TCAM capacity for each resource.

For more information about IPv4 and IPv6 protocol stacks, see the “Implementing IPv6 Addressing and Basic Connectivity” chapter of Cisco IOS IPv6 Configuration Guide on Cisco.com.

**DHCP for IPv6 Address Assignment**

DHCPv6 enables DHCP servers to pass configuration parameters, such as IPv6 network addresses, to IPv6 clients. The address assignment feature manages nonduplicate address assignment in the correct prefix based on the network where the host is connected. Assigned addresses can be from one or multiple prefix pools. Additional options, such as default domain and DNS name-server address, can be passed back to the client. Address pools can be assigned for use on a specific interface, on multiple interfaces, or the server can automatically find the appropriate pool.

This document describes only the DHCPv6 address assignment. For more information about configuring the DHCPv6 client, server, or relay agent functions, see the “Implementing DHCP for IPv6” chapter in the Cisco IOS IPv6 Configuration Guide on Cisco.com.

**Static Routes for IPv6**

Static routes are manually configured and define an explicit route between two networking devices. Static routes are useful for smaller networks with only one path to an outside network or to provide security for certain types of traffic in a larger network.

For more information about static routes, see the “Implementing Static Routes for IPv6” chapter in the Cisco IOS IPv6 Configuration Guide on Cisco.com.

**RIP for IPv6**

Routing Information Protocol (RIP) for IPv6 is a distance-vector protocol that uses hop count as a routing metric. It includes support for IPv6 addresses and prefixes and the all-RIP-routers multicast group address FF02::9 as the destination address for RIP update messages.

For more information about RIP for IPv6, see the “Implementing RIP for IPv6” chapter in the Cisco IOS IPv6 Configuration Guide on Cisco.com.

**OSPF for IPv6**

The switch supports Open Shortest Path First (OSPF) for IPv6, a link-state protocol for IP. For more information, see the “Implementing OSPF for IPv6” chapter in the Cisco IOS IPv6 Configuration Guide on Cisco.com.

**EIGRP for IPv6**

The switch supports Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6. It is configured on the interfaces on which it runs and does not require a global IPv6 address.

Before running, an instance of EIGRP IPv6 requires an implicit or explicit router ID. An implicit router ID is derived from a local IPv4 address, so any IPv4 node always has an available router ID. However, EIGRP IPv6 might be running in a network with only IPv6 nodes and therefore might not have an available IPv4 router ID.
For more information about EIGRP for IPv6, see the “Implementing EIGRP for IPv6” chapter in the Cisco IOS IPv6 Configuration Guide on Cisco.com.

**Multiprotocol BGP for IPv6**

Multiprotocol Border Gateway Protocol (BGP) is the supported exterior gateway protocol for IPv6. Multiprotocol BGP extensions for IPv6 support the same features and functionality as IPv4 BGP. IPv6 enhancements to multiprotocol BGP include support for IPv6 address family and network layer reachability information (NLRI) and next-hop (the next router in the path to the destination) attributes that use IPv6 addresses.

The switch does not support multicast BGP or non-stop forwarding (NSF) for IPv6 or for BGP IPv6.

For more information about configuring BGP for IPv6, see the “Implementing Multiprotocol BGP for IPv6” chapter in the Cisco IOS IPv6 Configuration Guide on Cisco.com.

**SNMP and Syslog Over IPv6**

To support both IPv4 and IPv6, IPv6 network management requires both IPv6 and IPv4 transports. Syslog over IPv6 supports address data types for these transports.

SNMP and syslog over IPv6 provide these features:

- Support for both IPv4 and IPv6
- IPv6 transport for SNMP and to modify the SNMP agent to support traps for an IPv6 host
- SNMP- and syslog-related MIBs to support IPv6 addressing
- Configuration of IPv6 hosts as trap receivers

For support over IPv6, SNMP modifies the existing IP transport mapping to simultaneously support IPv4 and IPv6. These SNMP actions support IPv6 transport management:

- Opens User Datagram Protocol (UDP) SNMP socket with default settings
- Provides a new transport mechanism called SR_IPV6_TRANSPORT
- Sends SNMP notifications over IPv6 transport
- Supports SNMP-named access lists for IPv6 transport
- Supports SNMP proxy forwarding using IPv6 transport
- Verifies SNMP Manager feature works with IPv6 transport

For information on SNMP over IPv6, including configuration procedures, see the “Managing Cisco IOS Applications over IPv6” chapter in the Cisco IOS IPv6 Configuration Guide on Cisco.com.

For information about syslog over IPv6, including configuration procedures, see the “Implementing IPv6 Addressing and Basic Connectivity” chapter in the Cisco IOS IPv6 Configuration Guide on Cisco.com.

**HTTP(S) Over IPv6**

The HTTP client sends requests to both IPv4 and IPv6 HTTP servers, which respond to requests from both IPv4 and IPv6 HTTP clients. URLs with literal IPv6 addresses must be specified in hexadecimal using 16-bit values between colons.

The accept socket call chooses an IPv4 or IPv6 address family. The accept socket is either an IPv4 or IPv6 socket. The listening socket continues to listen for both IPv4 and IPv6 signals that indicate a connection. The IPv6 listening socket is bound to an IPv6 wildcard address.
The underlying TCP/IP stack supports a dual-stack environment. HTTP relies on the TCP/IP stack and the sockets for processing network-layer interactions.

Basic network connectivity (ping) must exist between the client and the server hosts before HTTP connections can be made.

For more information, see the “Managing Cisco IOS Applications over IPv6” chapter in the Cisco IOS IPv6 Configuration Guide on Cisco.com.

### Unsupported IPv6 Unicast Routing Features

- IPv6 policy-based routing
- IPv6 virtual private network (VPN) routing and forwarding (VRF) table support
- Support for Intermediate System-to-Intermediate System (IS-IS) routing
- IPv6 packets destined to site-local addresses
- Tunneling protocols, such as IPv4-to-IPv6 or IPv6-to-IPv4
- The switch as a tunnel endpoint supporting IPv4-to-IPv6 or IPv6-to-IPv4 tunneling protocols
- IPv6 unicast reverse-path forwarding
- IPv6 general prefixes
- IPv6 HSRP

*Note*
The switch does not support IPv6-related features with any ES-port specific features, such as MPLS, EoMPLS, QinQ trust, or hierarchical QoS.

### Limitations

Because IPv6 is implemented in switch hardware, some limitations occur due to the IPv6 compressed addresses in the TCAM. These hardware limitations result in some loss of functionality and limits some features.

These are feature limitations.

- ICMPv6 redirect functionality is not supported for IPv6 host routes (routes used to reach a specific host) or for IPv6 routes with masks greater than 64 bits. The switch cannot redirect hosts to a better first-hop router for a specific destination that is reachable through a host route or through a route with masks greater than 64 bits.
- Load balancing using equal cost and unequal cost routes is not supported for IPv6 host routes or for IPv6 routes with a mask greater than 64 bits.
- The switch cannot forward SNAP-encapsulated IPv6 packets.

*Note*
There is a similar limitation for IPv4 SNAP-encapsulated packets, but the packets are dropped at the switch and are not forwarded.

- The switch routes IPv6-to-IPv4 and IPv4-to-IPv6 packets in hardware, but the switch cannot be an IPv6-to-IPv4 or IPv4-to-IPv6 tunnel endpoint.
• Bridged IPv6 packets with hop-by-hop extension headers are forwarded in software. In IPv4, these packets are routed in software, but bridged in hardware.

• In addition to the normal SPAN and RSPAN limitations defined in the software configuration guide, these limitations are specific to IPv6 packets:
  – When you send RSPAN IPv6-routed packets, the source MAC address in the SPAN output packet can be incorrect.
  – When you send RSPAN IPv6-routed packets, the destination MAC address can be incorrect. Normal traffic is not affected.

• The switch cannot apply QoS classification or policy-based routing on source-routed IPv6 packets in hardware.

• The switch cannot generate ICMPv6 Packet Too Big messages for multicast packets.

### Configuring IPv6

- Default IPv6 Configuration, page 37-9
- Configuring IPv6 Addressing and Enabling IPv6 Routing, page 37-10
- Configuring Default Router Preference, page 37-12
- Configuring IPv4 and IPv6 Protocol Stacks, page 37-12
- Configuring DHCP for IPv6 Address Assignment, page 37-14
- Configuring IPv6 ICMP Rate Limiting, page 37-17
- Configuring CEF for IPv6, page 37-18
- Configuring Static Routes for IPv6, page 37-18
- Configuring RIP for IPv6, page 37-20
- Configuring OSPF for IPv6, page 37-21
- Configuring EIGRP for IPv6, page 37-23
- Configuring BGP for IPv6, page 37-23

### Default IPv6 Configuration

Table 37-1 shows the default IPv6 configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDM template</td>
<td>Default</td>
</tr>
<tr>
<td>IPv6 routing</td>
<td>Disabled globally and on all interfaces.</td>
</tr>
<tr>
<td>CEFv6 or dCEFv6</td>
<td>Disabled (IPv4 CEF and dCEF are enabled by default).</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> When IPv6 routing is enabled, CEFv6 and dCEFv6 are automatically enabled.</td>
</tr>
<tr>
<td>IPv6 addresses</td>
<td>None configured.</td>
</tr>
</tbody>
</table>
Configuring IPv6 Addressing and Enabling IPv6 Routing

This section describes how to assign IPv6 addresses to individual Layer 3 interfaces and to globally forward IPv6 traffic on the switch.

Before configuring IPv6 on the switch, consider these guidelines:

- Be sure to select a dual IPv4 and IPv6 SDM template.
- See the “Unsupported IPv6 Unicast Routing Features” section on page 37-8 for IPv6 features that are not supported.
- In the `ipv6 address` interface configuration command, you must enter the `ipv6-address` and `ipv6-prefix` variables with the address specified in hexadecimal using 16-bit values between colons. The `prefix-length` variable (preceded by a slash `/`) is a decimal value that shows how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address).

To forward IPv6 traffic on an interface, you must configure a global IPv6 address on that interface. Configuring an IPv6 address on an interface automatically configures a link-local address and activates IPv6 for the interface. The configured interface automatically joins these required multicast groups for that link:

- solicited-node multicast group FF02:0:0:0:0:1:ff00::/104 for each unicast address assigned to the interface (this address is used in the neighbor discovery process.)
- all-nodes link-local multicast group FF02::1
- all-routers link-local multicast group FF02::2

For more information about configuring IPv6 routing, see the “Implementing Addressing and Basic Connectivity for IPv6” chapter in the *Cisco IOS IPv6 Configuration Guide* on Cisco.com.

Beginning in privileged EXEC mode, follow these steps to assign an IPv6 address to a Layer 3 interface and enable IPv6 routing:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>sdm prefer dual-ipv4-and-ipv6 {default</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>reload</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>no switchport</td>
</tr>
</tbody>
</table>
Step 8

**ipv6 address ipv6-prefix/prefix length eui-64**

Specify a global IPv6 address with an extended unique identifier (EUI) in the low-order 64 bits of the IPv6 address. Specify only the network prefix; the last 64 bits are automatically computed from the switch MAC address. This enables IPv6 processing on the interface.

**or**

**ipv6 address ipv6-address link-local**

Specify a link-local address on the interface to be used instead of the link-local address that is automatically configured when IPv6 is enabled on the interface. This command enables IPv6 processing on the interface.

**or**

**ipv6 enable**

Automatically configure an IPv6 link-local address on the interface, and enable the interface for IPv6 processing. The link-local address can only be used to communicate with nodes on the same link.

---

**Step 9**

**exit**

Return to global configuration mode.

**Step 10**

**ip routing**

Enable IP routing on the switch.

**Step 11**

**ipv6 unicast-routing**

Enable forwarding of IPv6 unicast data packets.

**Step 12**

**end**

Return to privileged EXEC mode.

**Step 13**

**show ipv6 interface interface-id**

Verify your entries.

**Step 14**

**copy running-config startup-config**

(Optional) Save your entries in the configuration file.

---

To remove an IPv6 address from an interface, use the **no ipv6 address ipv6-prefix/prefix length eui-64** or **no ipv6 address ipv6-address link-local** interface configuration command. To remove all manually configured IPv6 addresses from an interface, use the **no ipv6 address** interface configuration command without arguments. To disable IPv6 processing on an interface that has not been explicitly configured with an IPv6 address, use the **no ipv6 enable** interface configuration command. To globally disable IPv6 routing, use the **no ipv6 unicast-routing** global configuration command.

This example shows how to enable IPv6 with both a link-local address and a global address based on the IPv6 prefix 2001:0DB8:c18:1::/64. The EUI-64 interface ID is used in the low-order 64 bits of both addresses. Output from the **show ipv6 interface** EXEC command shows how the interface ID (20B:46FF:FE2F:D940) is appended to the link-local prefix FE80::/64 of the interface.

```
Switch(config)# sdm prefer dual-ipv4-and-ipv6 default
Switch(config)# ipv6 unicast-routing
Switch(config)# interface gigabitethernet1/1/1
Switch(config-if)# no switchport
Switch(config-if)# ipv6 address 2001:0DB8:c18:1::/64 eui 64
Switch(config-if)# end
Switch# show ipv6 interface gigabitethernet1/1/1
GigabitEthernet1/1/1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::20B:46FF:FE2F:D940
Global unicast address(es):
2001:0DB8:c18:1:20B:46FF:FE2F:D940, subnet is 2001:0DB8:c18:1::/64 [EUI] Joined group address(es):
FF02::1
FF02::2
FF02::1:FF2F:D940
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
```
Configuring Default Router Preference

Router advertisement messages are sent with the default router preference (DRP) configured by the `ipv6 nd router-preference` interface configuration command. If no DRP is configured, RAs are sent with a medium preference.

A DRP is useful when two routers on a link might provide equivalent, but not equal-cost routing, and policy might dictate that hosts should prefer one of the routers.

Beginning in privileged EXEC mode, follow these steps to configure a DRP for a router on an interface.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>ipv6 nd router-preference {high</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
</tr>
<tr>
<td>Step 5</td>
<td>show ipv6 interface</td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

Use the `no ipv6 nd router-preference` interface configuration command to disable an IPv6 DRP.

This example shows how to configure a DRP of `high` for the router on an interface.

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1/1
Switch(config-if)# ipv6 nd router-preference high
Switch(config-if)# end
```

For more information about configuring DRP for IPv6, see the “Implementing IPv6 Addresses and Basic Connectivity” chapter in the *Cisco IOS IPv6 Configuration Guide* on Cisco.com.

Configuring IPv4 and IPv6 Protocol Stacks

Before configuring IPv6 routing, you must select an SDM template that supports IPv4 and IPv6. If not already configured, use the `sdm prefer dual-ipv4-and-ipv6 {default | routing | vlan}` global configuration command to configure a template that supports IPv6. When you select a new template, you must reload the switch by using the `reload` privileged EXEC command so that the template takes effect.
Beginning in privileged EXEC mode, follow these steps to configure a Layer 3 interface to support both IPv4 and IPv6 and to enable IPv6 routing.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>sdm prefer dual-ipv4-and-ipv6 {default</td>
</tr>
<tr>
<td></td>
<td>• default—Set the switch to the default template to balance system resources.</td>
</tr>
<tr>
<td></td>
<td>• routing—Set the switch to the routing template to support IPv4 and IPv6 routing, including IPv4 policy-based routing.</td>
</tr>
<tr>
<td></td>
<td>• vlan—Maximize VLAN configuration on the switch with no routing supported in hardware.</td>
</tr>
<tr>
<td>Step 3</td>
<td>end Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>reload Reload the operating system.</td>
</tr>
<tr>
<td>Step 5</td>
<td>configure terminal Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 6</td>
<td>ip routing Enable routing on the switch.</td>
</tr>
<tr>
<td>Step 7</td>
<td>ipv6 unicast-routing Enable forwarding of IPv6 data packets on the switch.</td>
</tr>
<tr>
<td>Step 8</td>
<td>interface interface-id Enter interface configuration mode, and specify the Layer 3 interface to configure.</td>
</tr>
<tr>
<td>Step 9</td>
<td>no switchport Remove the interface from Layer 2 configuration mode (if it is a physical interface).</td>
</tr>
<tr>
<td>Step 10</td>
<td>ip address ip-address mask [secondary] Specify a primary or secondary IPv4 address for the interface.</td>
</tr>
<tr>
<td>Step 11</td>
<td>ipv6 address ipv6-prefix/prefix length eui-64 Specify a global IPv6 address. Specify only the network prefix; the last 64 bits are automatically computed from the switch MAC address.</td>
</tr>
<tr>
<td></td>
<td>or ipv6 address ipv6-address link-local Specify a link-local address on the interface to be used instead of the automatically configured link-local address when IPv6 is enabled on the interface.</td>
</tr>
<tr>
<td></td>
<td>or ipv6 enable Automatically configure an IPv6 link-local address on the interface, and enable the interface for IPv6 processing. The link-local address can only be used to communicate with nodes on the same link.</td>
</tr>
<tr>
<td>Step 12</td>
<td>end Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 13</td>
<td>show interface interface-id show ip interface interface-id show ipv6 interface interface-id Verify your entries.</td>
</tr>
<tr>
<td>Step 14</td>
<td>copy running-config startup-config (Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable IPv4 routing, use the no ip routing global configuration command. To disable IPv6 routing, use the no ipv6 unicast-routing global configuration command. To remove an IPv4 address from an interface, use the no ip address ip-address mask interface configuration command. To remove an IPv6 address from an interface, use the no ipv6 address ipv6-prefix/prefix length eui-64 or no ipv6 address ipv6-address link-local interface configuration command. To remove all manually configured IPv6
Configuring IPv6

addresses from an interface, use the **no ipv6 address** interface configuration command without arguments. To disable IPv6 processing on an interface that has not been explicitly configured with an IPv6 address, use the **no ipv6 enable** interface configuration command.

This example shows how to enable IPv4 and IPv6 routing on an interface.

```
Switch(config)# sdm prefer dual-ipv4-and-ipv6 default
Switch(config)# ip routing
Switch(config)# ipv6 unicast-routing
Switch(config)# interface gigabitethernet1/1/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 192.168.99.1 255.255.255.0
Switch(config-if)# ipv6 address 2001:0DB8:c18:1::/64 eui 64
Switch(config-if)# end
```

### Configuring DHCP for IPv6 Address Assignment

These sections describe how to configure Dynamic Host Configuration Protocol for IPv6 (DHCPv6) address assignment:

- Default DHCPv6 Address Assignment Configuration, page 37-14
- DHCPv6 Address Assignment Configuration Guidelines, page 37-14
- Enabling DHCPv6 Server Function, page 37-15
- Enabling DHCPv6 Client Function, page 37-17

### Default DHCPv6 Address Assignment Configuration

By default, no DHCPv6 features are configured on the switch.

### DHCPv6 Address Assignment Configuration Guidelines

When configuring DHCPv6 address assignment, consider these guidelines:

- In the procedures, the specified interface must be one of these Layer 3 interfaces:
  - DHCPv6 IPv6 routing must be enabled on a Layer 3 interface.
  - SVI: a VLAN interface created by using the `interface vlan vlan_id` command.
  - EtherChannel port channel in Layer 3 mode: a port-channel logical interface created by using the `interface port-channel port-channel-number` command.
- Before configuring DHCPv6, you must select a Switch Database Management (SDM) template that supports IPv4 and IPv6.
- The switch can act as a DHCPv6 client, server, or relay agent. The DHCPv6 client, server, and relay function are mutually exclusive on an interface.
Enabling DHCPv6 Server Function

Beginning in privileged EXEC mode, follow these steps to enable the DHCPv6 server function on an interface.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>ipv6 dhcp pool poolname Enter DHCP pool configuration mode, and define the name for the IPv6 DHCP pool. The pool name can be a symbolic string (such as Engineering) or an integer (such as 0).</td>
</tr>
<tr>
<td>Step 3</td>
<td>address prefix IPv6-prefix lifetime t1</td>
</tr>
<tr>
<td>Step 4</td>
<td>link-address IPv6-prefix (Optional) Specify a link-address IPv6 prefix. When an address on the incoming interface or a link-address in the packet matches the specified IPv6 prefix, the server uses the configuration information pool. This address must be in hexadecimal, using 16-bit values between colons.</td>
</tr>
<tr>
<td>Step 5</td>
<td>vendor-specific vendor-id (Optional) Enter vendor-specific configuration mode and enter a vendor-specific identification number. This number is the vendor IANA Private Enterprise Number. The range is 1 to 4294967295.</td>
</tr>
<tr>
<td>Step 6</td>
<td>suboption number [address IPv6-address</td>
</tr>
<tr>
<td>Step 7</td>
<td>exit Return to DHCP pool configuration mode.</td>
</tr>
<tr>
<td>Step 8</td>
<td>exit Return to global configuration mode.</td>
</tr>
<tr>
<td>Step 9</td>
<td>interface interface-id Enter interface configuration mode, and specify the interface to configure.</td>
</tr>
</tbody>
</table>
To delete a DHCPv6 pool, use the `no ipv6 dhcp pool poolname` global configuration command. Use the `no` form of the DHCP pool configuration mode commands to change the DHCPv6 pool characteristics.

To disable the DHCPv6 server function on an interface, use the `no ipv6 dhcp server interface` configuration command.

This example shows how to configure a pool called `engineering` with an IPv6 address prefix:

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool engineering
Switch(config-dhcpv6)# address prefix 2001:1000::/64
Switch(config-dhcpv6)#
```

This example shows how to configure a pool called `testgroup` with three link-addresses and an IPv6 address prefix:

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool testgroup
Switch(config-dhcpv6)# link-address 2001:1001::/64
Switch(config-dhcpv6)# link-address 2001:1002::/64
Switch(config-dhcpv6)# link-address 2001:2000::/48
Switch(config-dhcpv6)# address prefix 2001:1003::/64
Switch(config-dhcpv6)#
```

This example shows how to configure a pool called `350` with vendor-specific options:

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool 350
Switch(config-dhcpv6)# address prefix 2001:1005::/48
Switch(config-dhcpv6)# vendor-specific 9
Switch(config-dhcpv6)#
```

### Command Purpose

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`ipv6 dhcp server [poolname</td>
<td>automatic] [rapid-commit] [preference value] [allow-hint]`</td>
</tr>
<tr>
<td>- <code>poolname</code>—(Optional) User-defined name for the IPv6 DHCP pool. The pool name can be a symbolic string (such as Engineering) or an integer (such as 0).</td>
<td></td>
</tr>
<tr>
<td>- <code>automatic</code>—(Optional) Enables the system to automatically determine which pool to use when allocating addresses for a client.</td>
<td></td>
</tr>
<tr>
<td>- <code>rapid-commit</code>—(Optional) Allow two-message exchange method.</td>
<td></td>
</tr>
<tr>
<td>- <code>preference value</code>—(Optional) The preference value carried in the preference option in the advertise message sent by the server. The range is from 0 to 255. The preference value default is 0.</td>
<td></td>
</tr>
<tr>
<td>- <code>allow-hint</code>—(Optional) Specifies whether the server should consider client suggestions in the SOLICIT message. By default, the server ignores client hints.</td>
<td></td>
</tr>
<tr>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><code>show ipv6 dhcp pool</code> or <code>show ipv6 dhcp interface</code></td>
<td>Verify DHCPv6 pool configuration. Verify that the DHCPv6 server function is enabled on an interface.</td>
</tr>
<tr>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
Enabling DHCPv6 Client Function

Beginning in privileged EXEC mode, follow these steps to enable DHCPv6 client function on an interface.

```
Switch(config-dhcpv6-vs)# suboption 1 address 1000:235D::1
Switch(config-dhcpv6-vs)# suboption 2 ascii "IP-Phone"
Switch(config-dhcpv6-vs)# end
```

### Command Purpose

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>interface interface-id</td>
<td>Enter interface configuration mode, and specify the interface to configure.</td>
</tr>
</tbody>
</table>
| 3    | ipv6 address dhcp [rapid-commit] | Enable the interface to acquire an IPv6 address from the DHCPv6 server.  
**rapid-commit**—(Optional) Allow two-message exchange method for address assignment. |
| 4    | ipv6 dhcp client request [vendor-specific] | (Optional) Enable the interface to request the vendor-specific option. |
| 5    | end | Return to privileged EXEC mode. |
| 6    | show ipv6 dhcp interface | Verify that the DHCPv6 client is enabled on an interface. |

To disable the DHCPv6 client function, use the `no ipv6 address dhcp` interface configuration command. To remove the DHCPv6 client request, use the `no ipv6 address dhcp client request` interface configuration command.

This example shows how to acquire an IPv6 address and to enable the rapid-commit option:

```
Switch(config)# interface gigabitethernet 1/1/1
Switch(config-if)# ipv6 address dhcp rapid-commit
```

This document describes only the DHCPv6 address assignment. For more information about configuring the DHCPv6 client, server, or relay agent functions, see the “Implementing DHCP for IPv6” chapter in the *Cisco IOS IPv6 Configuration Guide* on Cisco.com.

### Configuring IPv6 ICMP Rate Limiting

ICMP rate limiting is enabled by default with a default interval between error messages of 100 milliseconds and a bucket size (maximum number of tokens to be stored in a bucket) of 10.
Beginning in privileged EXEC mode, follow these steps to change the ICMP rate-limiting parameters:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>ipv6 icmp error-interval</td>
<td>Configure the interval and bucket size for IPv6 ICMP error messages:</td>
</tr>
<tr>
<td></td>
<td>- interval—The interval (in milliseconds) between tokens</td>
</tr>
<tr>
<td></td>
<td>being added to the bucket. The range is from 0 to 2147483647</td>
</tr>
<tr>
<td></td>
<td>milliseconds.</td>
</tr>
<tr>
<td></td>
<td>- bucketsize—(Optional) The maximum number of tokens</td>
</tr>
<tr>
<td></td>
<td>stored in the bucket. The range is from 1 to 200.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>show ipv6 interface</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td>copy running-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
<tr>
<td>startup-config</td>
<td></td>
</tr>
</tbody>
</table>

To return to the default configuration, use the `no ipv6 icmp error-interval` global configuration command.

This example shows how to configure an IPv6 ICMP error message interval of 50 milliseconds and a bucket size of 20 tokens.

`Switch(config)#ipv6 icmp error-interval 50 20`

**Configuring CEF for IPv6**

Cisco Express Forwarding (CEF) is a Layer 3 IP switching technology to improve network performance. IPv6 CEF is disabled by default but are automatically enabled when you configure IPv6 routing.

To route IPv6 unicast packets, you must first globally configure IPv6 unicast packet forwarding by using the `ipv6 unicast-routing` global configuration command. You must configure an IPv6 address and IPv6 processing on an interface by using the `ipv6 address` interface configuration command.

To disable IPv6 CEF, use the `no ipv6 cef` global configuration command. To reenable IPv6 CEF or dCEF if it has been disabled, use the `ipv6 cef` global configuration command. You can verify the IPv6 state by entering the `show ipv6 cef` privileged EXEC command.

For more information about configuring CEF and dCEF, see the “Implementing IPv6 Addressing and Basic Connectivity” chapter in the *Cisco IOS IPv6 Configuration Guide* on Cisco.com.

**Configuring Static Routes for IPv6**

Before configuring a static IPv6 route, you must enable routing by using the `ip routing` global configuration command, enable the forwarding of IPv6 packets by using the `ipv6 unicast-routing` global configuration command, and enable IPv6 on at least one Layer 3 interface by configuring an IPv6 address on the interface.
Beginning in privileged EXEC mode, follow these steps to configure an IPv6 static route:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>ipv6 route ipv6-prefix/prefix length</td>
<td>Configure a static IPv6 route.</td>
</tr>
<tr>
<td>{ipv6-address</td>
<td>interface-id} [ipv6-address]} [administrative distance]</td>
</tr>
<tr>
<td>• ipv6-prefix—The IPv6 network that is the destination of the static route. It can also be a hostname when static host routes are configured.</td>
<td></td>
</tr>
<tr>
<td>• /prefix length—The length of the IPv6 prefix. A decimal value that shows how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.</td>
<td></td>
</tr>
<tr>
<td>• ipv6-address—The IPv6 address of the next hop that can be used to reach the specified network. The IPv6 address of the next hop need not be directly connected; recursion is done to find the IPv6 address of the directly connected next hop. The address must be specified in hexadecimal using 16-bit values between colons.</td>
<td></td>
</tr>
<tr>
<td>• interface-id—Specify direct static routes from point-to-point and broadcast interfaces. With point-to-point interfaces, there is no need to specify the IPv6 address of the next hop. With broadcast interfaces, you should always specify the IPv6 address of the next hop, or ensure that the specified prefix is assigned to the link, specifying a link-local address as the next hop. You can optionally specify the IPv6 address of the next hop to which packets are sent.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>show ipv6 static [ipv6-address</td>
<td>ipv6-prefix/prefix length] [interface interface-id] [recursive] [detail]</td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td>show ipv6 route static [updated]</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
To remove a configured static route, use the `no ipv6 route ipv6-prefix/prefix length [ipv6-address | interface-id [ipv6-address]] [administrative distance]` global configuration command.

This example shows how to configure a floating static route with an administrative distance of 130 to an interface:

```
Switch(config)# ipv6 route 2001:0DB8::/32 gigabitethernet1/1/1 130
```

For more information about configuring static IPv6 routing, see the “Implementing Static Routes for IPv6” chapter in the Cisco IOS IPv6 Configuration Guide on Cisco.com.

## Configuring RIP for IPv6

Before configuring the switch to run IPv6 RIP, you must enable routing by using the `ip routing` global configuration command, enable the forwarding of IPv6 packets by using the `ipv6 unicast-routing` global configuration command, and enable IPv6 on any Layer 3 interfaces on which IPv6 RIP is to be enabled.

Beginning in privileged EXEC mode, follow these required and optional steps to configure IPv6 RIP:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>ipv6 router rip name</code></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>maximum-paths number-paths</code></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>exit</code></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>interface interface-id</code></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>ipv6 rip name enable</code></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>`ipv6 rip name default-information {only</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><code>end</code></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td><code>show ipv6 rip [name] [interface interface-id] [database] [next-hops]</code></td>
</tr>
<tr>
<td>or</td>
<td><code>show ipv6 route rip [updated]</code></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td><code>copy running-config startup-config</code></td>
</tr>
</tbody>
</table>
To disable a RIP routing process, use the `no ipv6 router rip name` global configuration command. To disable the RIP routing process for an interface, use the `no ipv6 rip name` interface configuration command.

This example shows how to enable the RIP routing process `cisco` with a maximum of eight equal-cost routes and to enable it on an interface:

```
Switch(config)# ipv6 router rip cisco
Switch(config-router)# maximum-paths 8
Switch(config)# exit
Switch(config)# interface gigabitethernet1/1/1
Switch(config-if)# ipv6 rip cisco enable
```

For more information about configuring RIP routing for IPv6, see the “Implementing RIP for IPv6” chapter in the *Cisco IOS IPv6 Configuration Guide* on Cisco.com

### Configuring OSPF for IPv6

You can customize OSPF for IPv6 for your network. However, the defaults for OSPF in IPv6 are set to meet the requirements of most customers and features.

Follow these guidelines:

- Be careful when changing the defaults for IPv6 commands. Changing the defaults might adversely affect OSPF for the IPv6 network.
- Before you enable IPv6 OSPF on an interface, you must
  - Enable routing by using the `ip routing` global configuration command.
  - Enable the forwarding of IPv6 packets by using the `ipv6 unicast-routing` global configuration command.
  - Enable IPv6 on Layer 3 interfaces on which you are enabling IPv6 OSPF.

Beginning in privileged EXEC mode, follow these required and optional steps to configure IPv6 OSPF:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>ipv6 router ospf process-id</code></td>
<td>Enable OSPF router configuration mode for the process. The process ID is the number administratively assigned when enabling the OSPF for IPv6 routing process. It is locally assigned and can be a positive integer from 1 to 65535.</td>
</tr>
</tbody>
</table>
Step 3

**area area-id range [ipv6-prefix/prefix length] [advertise | not-advertise] [cost cost]**

(Optional) Consolidate and summarize routes at an area boundary.

- **area-id**—Identifier of the area about which routes are to be summarized. It can be specified as either a decimal value or as an IPv6 prefix.
- **ipv6-prefix/prefix length**—The destination IPv6 network and a decimal value that shows how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark (/) must precede the decimal value.
- **advertise**—(Optional) Set the address range status to advertise and to generate a Type 3 summary link-state advertisement (LSA).
- **not-advertise**—(Optional) Set the address range status to DoNotAdvertise. The Type 3 summary LSA is suppressed, and component networks remain hidden from other networks.
- **cost cost**—(Optional) Metric or cost for this summary route, which is used during OSPF SPF calculation to determine the shortest paths to the destination. The value can be 0 to 16777215.

Step 4

**maximum paths number-paths**

(Optional) Define the maximum number of equal-cost routes to the same destination that IPv6 OSPF should enter in the routing table. The range is from 1 to 64, and the default is 16.

Step 5

**exit**

Return to global configuration mode.

Step 6

**interface interface-id**

Enter interface configuration mode, and specify the Layer 3 interface to configure.

Step 7

**ipv6 ospf process-id area area-id [instance instance-id]**

Enable OSPF for IPv6 on the interface.

- **instance instance-id**—(Optional) Instance identifier.

Step 8

**end**

Return to privileged EXEC mode.

Step 9

**show ipv6 ospf [process-id] [area-id] interface [interface-id]**

Display information about OSPF interfaces.

or

**show ipv6 ospf [process-id] [area-id]**

Display general information about OSPF routing processes.

Step 10

**copy running-config startup-config**

(Optional) Save your entries in the configuration file.

To disable an OSPF routing process, use the no **ipv6 router ospf process-id** global configuration command. To disable the OSPF routing process for an interface, use the no **ipv6 ospf process-id area area-id** interface configuration command.

For more information about configuring OSPF routing for IPv6, see the “Implementing OSPF for IPv6” chapter in the Cisco IOS IPv6 Configuration Guide on Cisco.com.
Configuring EIGRP for IPv6

By default, EIGRP for IPv6 is disabled. You can configure EIGRP for IPv6 on an interface. After configuring the router and the interface for EIGRP, enter the no shutdown privileged EXEC command to start EIGRP.

Note

If EIGRP for IPv6 is not in shutdown mode, EIGRP might start running before you enter the EIGRP router-mode commands to configure the router and the interface.

To set an explicit router ID, use the show ipv6 eigrp command to see the configured router IDs, and then use the router-id command.

As with EIGRP IPv4, you can use EIGRPv6 to specify your EIGRP IPv4 interfaces and to select a subset of those as passive interfaces. Use the passive-interface default command to make all interfaces passive, and then use the no passive-interface command on selected interfaces to make them active. You do not need to configure EIGRP IPv6 on a passive interface.

For more configuration procedures, see the “Implementing EIGRP for IPv6” chapter in the Cisco IOS IPv6 Configuration Guide on Cisco.com.

Configuring BGP for IPv6

When configuring multiprotocol BGP extensions for IPv6, you must create the BGP routing process, configure peering relationships, and customize BGP for your particular network. Note that BGP functions the same in IPv6 as in IPv4. Before configuring the router to run BGP for IPv6, you must use the ipv6 unicast-routing command to globally enable IPv6 routing.

Beginning in privileged EXEC mode, follow these steps to configure IPv6 BGP:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 router bgp as-number</td>
<td>Configure a BGP routing process, and enter BGP router configuration mode for the autonomous system number.</td>
</tr>
<tr>
<td>Step 3 no bgp default ipv4-unicast</td>
<td>Disable the IPv4 unicast address family for the BGP routing process specified in the previous step. Routing information for the IPv4 unicast address family is advertised by default for each BGP routing session unless you enter this command before configuring the neighbor remote-as command.</td>
</tr>
<tr>
<td>Step 4 bgp router-id ip-address</td>
<td>(Optional) Configure a fixed 32-bit router ID as the identifier of the local router running BGP. By default, the router ID is the IPv4 address of a router loopback interface. On a router enabled only for IPv6 (no IPv4 address), you must manually configure the BGP router ID. Note Configuring a router ID by using this command resets all active BGP peering sessions.</td>
</tr>
</tbody>
</table>
Displaying IPv6

For more configuration procedures, see the “Implementing Multiprotocol BGP for IPv6” chapter in the Cisco IOS IPv6 Configuration Guide on Cisco.com.


The switch does not support multicast IPv6 BGP, nonstop forwarding (NSF) for IPv6 BGP, 6PE multipath (EoMPLS), or IPv6 VRF.

Displaying IPv6

For complete syntax and usage information on these commands, see the Cisco IOS command reference publications.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show bgp ipv6</td>
<td>Display BGP IPv6 configuration and routing tables.</td>
</tr>
<tr>
<td>show ipv6 access-list</td>
<td>Display a summary of access lists.</td>
</tr>
<tr>
<td>show ipv6 cef</td>
<td>Display Cisco Express Forwarding for IPv6.</td>
</tr>
<tr>
<td>show ipv6 interface</td>
<td>Display IPv6 interface status and configuration.</td>
</tr>
<tr>
<td>show ipv6 mtu</td>
<td>Display IPv6 MTU per destination cache.</td>
</tr>
<tr>
<td>show ipv6 neighbors</td>
<td>Display IPv6 neighbor cache entries.</td>
</tr>
<tr>
<td>show ipv6 ospf</td>
<td>Display IPv6 OSPF information.</td>
</tr>
<tr>
<td>show ipv6 prefix-list</td>
<td>Display a list of IPv6 prefix lists.</td>
</tr>
<tr>
<td>show ipv6 protocols</td>
<td>Display IPv6 routing protocols on the switch.</td>
</tr>
<tr>
<td>show ipv6 rip</td>
<td>Display IPv6 RIP routing protocol status.</td>
</tr>
<tr>
<td>show ipv6 route</td>
<td>Display the IPv6 route table entries.</td>
</tr>
<tr>
<td>show ipv6 routers</td>
<td>Display the local IPv6 routers.</td>
</tr>
<tr>
<td>show ipv6 static</td>
<td>Display IPv6 static routes.</td>
</tr>
<tr>
<td>show ipv6 traffic</td>
<td>Display IPv6 traffic statistics.</td>
</tr>
</tbody>
</table>
Table 37-3  Commands for Displaying EIGRP IPv6 Information

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ipv6 eigrp [as-number] interface</code></td>
<td>Displays information about interfaces configured for EIGRP IPv6.</td>
</tr>
<tr>
<td><code>show ipv6 eigrp [as-number] neighbor</code></td>
<td>Displays the neighbors discovered by EIGRP IPv6.</td>
</tr>
<tr>
<td><code>show ipv6 eigrp [as-number] traffic</code></td>
<td>Displays the number of EIGRP IPv6 packets sent and received.</td>
</tr>
<tr>
<td>`show ipv6 eigrp topology [as-number</td>
<td>Displays EIGRP entries in the IPv6 topology table.</td>
</tr>
<tr>
<td>ipv6-address] [active</td>
<td>all-links</td>
</tr>
</tbody>
</table>

Table 37-4  Commands for Displaying IPv4 and IPv6 Address Types

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip http server history</code></td>
<td>Display the previous 20 connections to the HTTP server, including the IP address accessed and the time when the connection was closed.</td>
</tr>
<tr>
<td><code>show ip http server connection</code></td>
<td>Display the current connections to the HTTP server, including the local and remote IP addresses being accessed.</td>
</tr>
<tr>
<td><code>show ip http client connection</code></td>
<td>Display the configuration values for HTTP client connections to HTTP servers.</td>
</tr>
<tr>
<td><code>show ip http client history</code></td>
<td>Display a list of the last 20 requests made by the HTTP client to the server.</td>
</tr>
</tbody>
</table>

This is an example of the output from the `show ipv6 interface` privileged EXEC command:

```
Switch# show ipv6 interface
Vlan1 is up, line protocol is up
   IPv6 is enabled, link-local address is FE80::20B:46FF:FE2F:D940
   Global unicast address(es):
     3FFE:C000:0:1:20B:46FF:FE2F:D940, subnet is 3FFE:C000:0:1::/64 [EUI]
   Joined group address(es):
     FF02::1
     FF02::2
     FF02::1:FF2F:D940
   MTU is 1500 bytes
   ICMP error messages limited to one every 100 milliseconds
   ICMP redirects are enabled
   ND DAD is enabled, number of DAD attempts: 1
   ND reachable time is 30000 milliseconds
   ND advertised reachable time is 0 milliseconds
   ND advertised retransmit interval is 0 milliseconds
   ND router advertisements are sent every 200 seconds
   ND router advertisements live for 1800 seconds
<output truncated>
```

This is an example of the output from the `show ipv6 cef` privileged EXEC command:

```
Switch# show ipv6 cef
::/0
   nexthop 3FFE:C000:0:7::777 Vlan7
3FFE:C000:0:1::/64
   attached to Vlan1
3FFE:C000:0:1:20B:46FF:FE2F:D940/128
   receive
3FFE:C000:0:7::/64
   attached to Vlan7
```
Displaying IPv6

3FFE:C000:0:7::777/128
  attached to Vlan7
3FFE:C000:0:7:20B:46FF:FE2F:D97F/128
  receive
3FFE:C000:111:1::/64
  attached to FastEthernet1/0/11
3FFE:C000:111:1:20B:46FF:FE2F:D945/128
  receive
3FFE:C000:168:1::/64
  attached to FastEthernet2/0/43
3FFE:C000:168:1:20B:46FF:FE2F:D94B/128
  receive
3FFE:C000:16A:1::/64
  attached to Loopback10
3FFE:C000:16A:1:20B:46FF:FE2F:D900/128
  receive
&lt;output truncated&gt;

This is an example of the output from the `show ipv6 protocols` privileged EXEC command:

Switch# `show ipv6 protocols`
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "static"
IPv6 Routing Protocol is "rip fer"
Interfaces:
  Vlan6
  GigabitEthernet1/1/1
  GigabitEthernet1/1/2
Redistribution:
  None

This is an example of the output from the `show ipv6 rip` privileged EXEC command:

Switch# `show ipv6 rip`
RIP process "fer", port 521, multicast-group FF02::9, pid 190
  Administrative distance is 120. Maximum paths is 16
  Updates every 30 seconds, expire after 180
  Holddown lasts 0 seconds, garbage collect after 120
  Split horizon is on; poison reverse is off
  Default routes are not generated
  Periodic updates 9040, trigger updates 60

  Interfaces:
    Vlan6
    FastEthernet2/0/4
    FastEthernet2/0/11
    FastEthernet1/0/12
Redistribution:
  None

This is an example of the output from the `show ipv6 static` privileged EXEC command:

Switch# `show ipv6 static`
IPv6 Static routes
  Code: * - installed in RIB
  * ::/0 via nexthop 3FFE:C000:0:7::777, distance 1

This is an example of the output from the `show ipv6 neighbor` privileged EXEC command:

Switch# `show ipv6 neighbors`
IPv6 Address          Age    Link-layer Addr  State  Interface
3FFE:C000:0:7::777    -      0007.0007.0007  REACH  Vl7
3FFE:C101:113:1::33    -      0000.0000.0033  REACH  Fa1/0/13
This is an example of the output from the **show ipv6 route** privileged EXEC command:

```
Switch# show ipv6 route
IPv6 Routing Table - Default - 1 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
L  FF00::/8 [0/0]
   via Null0, receive
```

This is an example of the output from the **show ipv6 traffic** privileged EXEC command.

```
Switch# show ipv6 traffic
IPv6 statistics:
  Rcvd: 1 total, 1 local destination
    0 source-routed, 0 truncated
    0 format errors, 0 hop count exceeded
    0 bad header, 0 unknown option, 0 bad source
    0 unknown protocol, 0 not a router
    0 fragments, 0 total reassembled
    0 reassembly timeouts, 0 reassembly failures
  Sent: 36861 generated, 0 forwarded
    0 fragmented into 0 fragments, 0 failed
    0 encapsulation failed, 0 no route, 0 too big
    0 RPF drops, 0 RPF suppressed drops
Mcast: 1 received, 36861 sent

ICMP statistics:
  Rcvd: 1 input, 0 checksum errors, 0 too short
    0 unknown info type, 0 unknown error type
    unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
    parameter: 0 error, 0 header, 0 option
    0 hopcount expired, 0 reassembly timeout, 0 too big
    0 echo request, 0 echo reply
    0 group query, 0 group report, 0 group reduce
    1 router solicit, 0 router advert, 0 redirects
    0 neighbor solicit, 0 neighbor advert
  Sent: 10112 output, 0 rate-limited
    unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
    parameter: 0 error, 0 header, 0 option
    0 hopcount expired, 0 reassembly timeout, 0 too big
    0 echo request, 0 echo reply
    0 group query, 0 group report, 0 group reduce
    0 router solicit, 9944 router advert, 0 redirects
    84 neighbor solicit, 84 neighbor advert

UDP statistics:
  Rcvd: 0 input, 0 checksum errors, 0 length errors
    0 no port, 0 dropped
  Sent: 26749 output

TCP statistics:
  Rcvd: 0 input, 0 checksum errors
  Sent: 0 output, 0 retransmitted
```
Configuring IPv6 MLD Snooping

You can use Multicast Listener Discovery (MLD) snooping on the Catalyst 3750 Metro switch to enable efficient distribution of IP version 6 (IPv6) multicast data to clients and routers in a switched network.

Note
To use IPv6, you must configure the dual IPv4 and IPv6 Switch Database Management (SDM) template on the switch. You select the template by entering the `sdm prefer dual-ipv4-and-ipv6` global configuration command.

For related information, see these chapters:
- For more information about SDM templates, see Chapter 6, “Configuring SDM Templates.”
- For information about IPv6 on the switch, see Chapter 37, “Configuring IPv6 Unicast Routing.”

Note
For complete syntax and usage information for the commands used in this chapter, see the command reference for this release or the Cisco IOS documentation referenced in the procedures.

This chapter includes these sections:
- “Understanding MLD Snooping” section on page 38-1
- “Configuring IPv6 MLD Snooping” section on page 38-5
- “Displaying MLD Snooping Information” section on page 38-11

Understanding MLD Snooping

In IP version 4 (IPv4), Layer 2 switches can use Internet Group Management Protocol (IGMP) snooping to limit the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded to only those interfaces associated with IP multicast devices. In IPv6, MLD snooping performs a similar function. With MLD snooping, IPv6 multicast data is selectively forwarded to a list of ports that want to receive the data, instead of being flooded to all ports in a VLAN. This list is constructed by snooping IPv6 multicast control packets.

MLD is a protocol used by IPv6 multicast routers to discover the presence of multicast listeners (nodes wishing to receive IPv6 multicast packets) on its directly attached links and to discover which multicast packets are of interest to neighboring nodes. MLD is derived from IGMP; MLD version 1 (MLDv1) is equivalent to IGMPv2 and MLD version 2 (MLDv2) is equivalent to IGMPv3. MLD is a subprotocol of Internet Control Message Protocol version 6 (ICMPv6), and MLD messages are a subset of ICMPv6 messages, identified in IPv6 packets by a preceding Next Header value of 58.
The switch supports two versions of MLD snooping:

- MLDv1 snooping detects MLDv1 control packets and sets up traffic bridging based on IPv6 destination multicast addresses.
- MLDv2 basic snooping (MBSS) uses MLDv2 control packets to set up traffic forwarding based on IPv6 destination multicast addresses.

The switch can snoop on both MLDv1 and MLDv2 protocol packets and bridge IPv6 multicast data based on destination IPv6 multicast addresses.

**Note**

The switch does not support MLDv2 enhanced snooping (MESS), which sets up IPv6 source and destination multicast address-based forwarding.

MLD snooping can be enabled or disabled globally or per VLAN. When MLD snooping is enabled, a per-VLAN IPv6 multicast MAC address table is constructed in software and a per-VLAN IPv6 multicast address table is constructed in software and hardware. The switch then performs IPv6 multicast-address based bridging in hardware.

These sections describe some parameters of IPv6 MLD snooping:

- MLD Messages, page 38-2
- MLD Queries, page 38-2
- Multicast Client Aging Robustness, page 38-3
- Multicast Router Discovery, page 38-3
- MLD Reports, page 38-4
- MLD Done Messages and Immediate-Leave, page 38-4
- Topology Change Notification Processing, page 38-4

### MLD Messages

MLDv1 supports three types of messages:

- Listener Queries are the equivalent of IGMPv2 queries and are either General Queries or Multicast-Address-Specific Queries (MASQs).
- Multicast Listener Reports are the equivalent of IGMPv2 reports.
- Multicast Listener Done messages are the equivalent of IGMPv2 leave messages.

MLDv2 supports MLDv2 queries and reports, as well as MLDv1 Report and Done messages.

Message timers and state transitions resulting from messages being sent or received are the same as those of IGMPv2 messages. MLD messages that do not have valid link-local IPv6 source addresses are ignored by MLD routers and switches.

### MLD Queries

The switch sends out MLD queries, constructs an IPv6 multicast address database, and generates MLD group-specific and MLD group-and-source-specific queries in response to MLD Done messages. The switch also supports report suppression, report proxying, Immediate-Leave functionality, and static IPv6 multicast MAC-address configuration.
When MLD snooping is disabled, all MLD queries are flooded in the ingress VLAN.

When MLD snooping is enabled, received MLD queries are flooded in the ingress VLAN, and a copy of the query is sent to the CPU for processing. From the received query, MLD snooping builds the IPv6 multicast address database. It detects multicast router ports, maintains timers, sets report response time, learns the querier IP source address for the VLAN, learns the querier port in the VLAN, and maintains multicast-address aging.

**Note**

When the IPv6 multicast router is a Catalyst 6500 switch and you are using extended VLANs (in the range 1006 to 4094), IPv6 MLD snooping must be enabled on the extended VLAN on the Catalyst 6500 switch in order for this switch to receive queries on the VLAN. For normal-range VLANs (1 to 1005), it is not necessary to enable IPv6 MLD snooping on the VLAN on the Catalyst 6500 switch.

When a group exists in the MLD snooping database, the switch responds to a group-specific query by sending an MLDv1 report. When the group is unknown, the group-specific query is flooded to the ingress VLAN.

When a host wants to leave a multicast group, it can send out an MLD Done message (equivalent to IGMP Leave message). When the switch receives an MLDv1 Done message, if Immediate-Leave is not enabled, the switch sends an MASQ to the port from which the message was received to determine if other devices connected to the port should remain in the multicast group.

### Multicast Client Aging Robustness

You can configure port membership removal from addresses based on the number of queries. A port is removed from membership to an address only when there are no reports to the address on the port for the configured number of queries. The default number is 2.

### Multicast Router Discovery

Like IGMP snooping, MLD snooping performs multicast router discovery, with these characteristics:

- Ports configured by a user never age out.
- Dynamic port learning results from MLDv1 snooping queries and IPv6 PIMv2 packets.
- If there are multiple routers on the same Layer 2 interface, MLD snooping tracks a single multicast router on the port (the router that most recently sent a router control packet).
- Dynamic multicast router port aging is based on a default timer of 5 minutes; the multicast router is deleted from the router port list if no control packet is received on the port for 5 minutes.
- IPv6 multicast router discovery only takes place when MLD snooping is enabled on the switch.
- Received IPv6 multicast router control packets are always flooded to the ingress VLAN, whether or not MLD snooping is enabled on the switch.
- After the discovery of the first IPv6 multicast router port, unknown IPv6 multicast data is forwarded only to the discovered router ports (before that time, all IPv6 multicast data is flooded to the ingress VLAN).
MLD Reports

The processing of MLDv1 join messages is essentially the same as with IGMPv2. When no IPv6 multicast routers are detected in a VLAN, reports are not processed or forwarded from the switch. When IPv6 multicast routers are detected and an MLDv1 report is received, an IPv6 multicast group address and an IPv6 multicast MAC address are entered in the VLAN MLD database. Then all IPv6 multicast traffic to the group within the VLAN is forwarded using this address. When MLD snooping is disabled, reports are flooded in the ingress VLAN.

When MLD snooping is enabled, MLD report suppression, called listener message suppression, is automatically enabled. With report suppression, the switch forwards the first MLDv1 report received by a group to IPv6 multicast routers; subsequent reports for the group are not sent to the routers. When MLD snooping is disabled, report suppression is disabled, and all MLDv1 reports are flooded to the ingress VLAN.

The switch also supports MLDv1 proxy reporting. When an MLDv1 MASQ is received, the switch responds with MLDv1 reports for the address on which the query arrived if the group exists in the switch on another port and if the port on which the query arrived is not the last member port for the address.

MLD Done Messages and Immediate-Leave

When the Immediate-Leave feature is enabled and a host sends an MLDv1 Done message (equivalent to an IGMP leave message), the port on which the Done message was received is immediately deleted from the group. You enable Immediate-Leave on VLANs and (as with IGMP snooping), you should only use the feature on VLANs where a single host is connected to the port. If the port was the last member of a group, the group is also deleted, and the leave information is forwarded to the detected IPv6 multicast routers.

When Immediate Leave is not enabled in a VLAN (which would be the case when there are multiple clients for a group on the same port) and a Done message is received on a port, an MASQ is generated on that port. The user can control when a port membership is removed for an existing address in terms of the number of MASQs. A port is removed from membership to an address when there are no MLDv1 reports to the address on the port for the configured number of queries.

The number of MASQs generated is configured by using the `ipv6 mld snooping last-listener-query count` global configuration command. The default number is 2.

The MASQ is sent to the IPv6 multicast address for which the Done message was sent. If there are no reports sent to the IPv6 multicast address specified in the MASQ during the switch maximum response time, the port on which the MASQ was sent is deleted from the IPv6 multicast address database. The maximum response time is the time configured by using the `ipv6 mld snooping last-listener-query-interval` global configuration command. If the deleted port is the last member of the multicast address, the multicast address is also deleted, and the switch sends the address leave information to all detected multicast routers.

Topology Change Notification Processing

When topology change notification (TCN) solicitation is enabled by using the `ipv6 mld snooping tcn query solicit` global configuration command, MLDv1 snooping sets the VLAN to flood all IPv6 multicast traffic with a configured number of MLDv1 queries before it begins sending multicast data only to selected ports. You set this value by using the `ipv6 mld snooping tcn flood query count` global
configuration command. The default is to send two queries. The switch also generates MLDv1 global Done messages with valid link-local IPv6 source addresses when the switch becomes the STP root in the VLAN or when it is configured by the user. This is same as done in IGMP snooping.

**Configuring IPv6 MLD Snooping**

These sections describe how to configure IPv6 MLD snooping:

- Default MLD Snooping Configuration, page 38-5
- MLD Snooping Configuration Guidelines, page 38-6
- Enabling or Disabling MLD Snooping, page 38-6
- Configuring a Static Multicast Group, page 38-7
- Configuring a Multicast Router Port, page 38-8
- Enabling MLD Immediate Leave, page 38-8
- Configuring MLD Snooping Queries, page 38-9
- Disabling MLD Listener Message Suppression, page 38-10

**Default MLD Snooping Configuration**

Table 38-1 shows the default MLD snooping configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>MLD snooping (Global)</td>
<td>Disabled.</td>
</tr>
<tr>
<td>MLD snooping (per VLAN)</td>
<td>Enabled. MLD snooping must be globally enabled for VLAN MLD snooping to take place.</td>
</tr>
<tr>
<td>IPv6 Multicast addresses</td>
<td>None configured.</td>
</tr>
<tr>
<td>IPv6 Multicast router ports</td>
<td>None configured.</td>
</tr>
<tr>
<td>MLD snooping Immediate Leave</td>
<td>Disabled.</td>
</tr>
<tr>
<td>MLD snooping robustness variable</td>
<td>Global: 2; Per VLAN: 0.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The VLAN value overrides the global setting. When the VLAN value is 0, the VLAN uses the global count.</td>
</tr>
<tr>
<td>Last listener query count</td>
<td>Global: 2; Per VLAN: 0.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The VLAN value overrides the global setting. When the VLAN value is 0, the VLAN uses the global count.</td>
</tr>
<tr>
<td>Last listener query interval</td>
<td>Global: 1000 (1 second); VLAN: 0.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The VLAN value overrides the global setting. When the VLAN value is 0, the VLAN uses the global count.</td>
</tr>
<tr>
<td>TCN query solicit</td>
<td>Disabled.</td>
</tr>
<tr>
<td>TCN query count</td>
<td>2.</td>
</tr>
<tr>
<td>MLD listener suppression</td>
<td>Enabled.</td>
</tr>
</tbody>
</table>
MLD Snooping Configuration Guidelines

When configuring MLD snooping, consider these guidelines:

- You can configure MLD snooping characteristics at any time, but you must globally enable MLD snooping by using the `ipv6 mld snooping` global configuration command for the configuration to take effect.

- When the IPv6 multicast router is a Catalyst 6500 switch and you are using extended VLANs (in the range 1006 to 4094), IPv6 MLD snooping must be enabled on the extended VLAN on the Catalyst 6500 switch in order for this switch to receive queries on the VLAN. For normal-range VLANs (1 to 1005), it is not necessary to enable IPv6 MLD snooping on the VLAN on the Catalyst 6500 switch.

- MLD snooping and IGMP snooping act independently of each other. You can enable both features at the same time on the switch.

- The maximum number of multicast entries allowed on the switch is determined by the configured SDM template.

- The maximum number of address entries allowed for the switch is 1000.

Enabling or Disabling MLD Snooping

By default, IPv6 MLD snooping is globally disabled on the switch and enabled on all VLANs. When MLD snooping is globally disabled, it is also disabled on all VLANs. When you globally enable MLD snooping, the VLAN configuration overrides the global configuration. That is, MLD snooping is enabled only on VLAN interfaces in the default state (enabled).

You can enable and disable MLD snooping on a per-VLAN basis or for a range of VLANs, but if you globally disable MLD snooping, it is disabled in all VLANs. If global snooping is enabled, you can enable or disable VLAN snooping.

Beginning in privileged EXEC mode, follow these steps to globally enable MLD snooping on the switch:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: <code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2: <code>ipv6 mld snooping</code></td>
<td>Globally enable MLD snooping on the switch.</td>
</tr>
<tr>
<td>Step 3: <code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4: <code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
<tr>
<td>Step 5: <code>reload</code></td>
<td>Reload the operating system.</td>
</tr>
</tbody>
</table>

To globally disable MLD snooping on the switch, use the `no ipv6 mld snooping` global configuration command.

Beginning in privileged EXEC mode, follow these steps to enable MLD snooping on a VLAN.

Note

When the IPv6 multicast router is a Catalyst 6500 switch and you are using extended VLANs (in the range 1006 to 4094), IPv6 MLD snooping must be enabled on the extended VLAN on the Catalyst 6500 switch in order for this switch to receive queries on the VLAN. For normal-range VLANs (1 to 1005), it is not necessary to enable IPv6 MLD snooping on the VLAN on the Catalyst 6500 switch.
**Chapter 38  Configuring IPv6 MLD Snooping**

**Configuring IPv6 MLD Snooping**

To disable MLD snooping on a VLAN interface, use the `no ipv6 mld snooping vlan vlan-id` global configuration command for the specified VLAN number.

**Configuring a Static Multicast Group**

Hosts or Layer 2 ports normally join multicast groups dynamically, but you can also statically configure an IPv6 multicast address and member ports for a VLAN.

Beginning in privileged EXEC mode, follow these steps to add a Layer 2 port as a member of a multicast group:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>ipv6 mld snooping</code></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>ipv6 mld snooping vlan vlan-id</code></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>copy running-config startup-config</code></td>
</tr>
</tbody>
</table>

To remove a Layer 2 port from the multicast group, use the `no ipv6 mld snooping vlan vlan-id static mac-address interface interface-id` global configuration command. If all member ports are removed from a group, the group is deleted.
This example shows how to statically configure an IPv6 multicast group:

Switch# configure terminal
Switch(config)# ipv6 mld snooping vlan 2 static FF12::3 interface gigabitethernet1/1/1
Switch(config)# end

Configuring a Multicast Router Port

Although MLD snooping learns about router ports through MLD queries and PIMv6 queries, you can also use the command-line interface (CLI) to add a multicast router port to a VLAN. To add a multicast router port (add a static connection to a multicast router), use the `ipv6 mld snooping vlan mrouter` global configuration command on the switch.

Note

Static connections to multicast routers are supported only on switch ports.

Beginning in privileged EXEC mode, follow these steps to add a multicast router port to a VLAN:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>ipv6 mld snooping vlan vlan-id mrouter interface interface-id</code></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>end</code></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>show ipv6 mld snooping mrouter [vlan vlan-id]</code></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>copy running-config startup-config</code></td>
</tr>
</tbody>
</table>

To remove a multicast router port from the VLAN, use the `no ipv6 mld snooping vlan vlan-id mrouter interface interface-id` global configuration command.

This example shows how to add a multicast router port to VLAN 200:

Switch# configure terminal
Switch(config)# ipv6 mld snooping vlan 200 mrouter interface gigabitethernet1/1/2
Switch(config)# exit

Enabling MLD Immediate Leave

When you enable MLDv1 Immediate Leave, the switch immediately removes a port from a multicast group when it detects an MLD Done message on that port. You should only use the Immediate-Leave feature when there is a single receiver present on every port in the VLAN. When there are multiple clients for a multicast group on the same port, you should not enable Immediate-Leave in a VLAN.
Beginning in privileged EXEC mode, follow these steps to enable MLDv1 Immediate Leave:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>ipv6 mld snooping vlan vlan-id immediate-leave</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
</tr>
<tr>
<td>Step 4</td>
<td>show ipv6 mld snooping vlan vlan-id</td>
</tr>
<tr>
<td>Step 5</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To disable MLD Immediate Leave on a VLAN, use the `no ipv6 mld snooping vlan vlan-id immediate-leave` global configuration command.

This example shows how to enable MLD Immediate Leave on VLAN 130:

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping vlan 130 immediate-leave
Switch(config)# exit
```

### Configuring MLD Snooping Queries

When Immediate Leave is not enabled and a port receives an MLD Done message, the switch generates MASQs on the port and sends them to the IPv6 multicast address for which the Done message was sent. You can optionally configure the number of MASQs that are sent and the length of time the switch waits for a response before deleting the port from the multicast group.

Beginning in privileged EXEC mode, follow these steps to configure MLD snooping query characteristics for the switch or for a VLAN:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>ipv6 mld snooping robustness-variable value</td>
</tr>
<tr>
<td>Step 3</td>
<td>ipv6 mld snooping vlan vlan-id robustness-variable value</td>
</tr>
<tr>
<td>Step 4</td>
<td>ipv6 mld snooping last-listener-query-count count</td>
</tr>
<tr>
<td>Step 5</td>
<td>ipv6 mld snooping vlan vlan-id last-listener-query-count count</td>
</tr>
</tbody>
</table>
Chapter 38 Configuring IPv6 MLD Snooping

### Command Purpose

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 6</td>
<td><code>ipv6 mld snooping last-listener-query-interval interval</code></td>
<td>(Optional) Set the maximum response time that the switch waits after sending out a MASQ before deleting a port from the multicast group. The range is 100 to 32,768 thousands of a second. The default is 1000 (1 second).</td>
</tr>
<tr>
<td>Step 7</td>
<td><code>ipv6 mld snooping vlan vlan-id last-listener-query-interval interval</code></td>
<td>(Optional) Set the last-listener query interval on a VLAN basis. This value overrides the value configured globally. The range is 0 to 32,768 thousands of a second. The default is 0. When set to 0, the global last-listener query interval is used.</td>
</tr>
<tr>
<td>Step 8</td>
<td><code>ipv6 mld snooping tcn query solicit</code></td>
<td>(Optional) Enable topology change notification (TCN) solicitation, which means that VLANs flood all IPv6 multicast traffic for the configured number of queries before sending multicast data to only those ports requesting to receive it. The default is for TCN to be disabled.</td>
</tr>
<tr>
<td>Step 9</td>
<td><code>ipv6 mld snooping tcn flood query count count</code></td>
<td>(Optional) When TCN is enabled, specify the number of TCN queries to be sent. The range is from 1 to 10; the default is 2.</td>
</tr>
<tr>
<td>Step 10</td>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 11</td>
<td><code>show ipv6 mld snooping querier [vlan vlan-id]</code></td>
<td>(Optional) Verify that the MLD snooping querier information for the switch or for the VLAN.</td>
</tr>
<tr>
<td>Step 12</td>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

This example shows how to set the MLD snooping global robustness variable to 3:

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping robustness-variable 3
Switch(config)# exit
```

This example shows how to set the MLD snooping last-listener query count for a VLAN to 3:

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping vlan 200 last-listener-query-count 3
Switch(config)# exit
```

This example shows how to set the MLD snooping last-listener query interval (maximum response time) to 2000 (2 seconds):

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping last-listener-query-interval 2000
Switch(config)# exit
```

### Disabling MLD Listener Message Suppression

MLD snooping listener message suppression is enabled by default. When it is enabled, the switch forwards only one MLD report per multicast router query. When message suppression is disabled, multiple MLD reports could be forwarded to the multicast routers.
Beginning in privileged EXEC mode, follow these steps to disable MLD listener message suppression:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>no ipv6 mld snooping listener-message-suppression</td>
<td>Disable MLD message suppression.</td>
</tr>
<tr>
<td>3</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>4</td>
<td>show ipv6 mld snooping</td>
<td>Verify that IPv6 MLD snooping report suppression is disabled.</td>
</tr>
<tr>
<td>5</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To re-enable MLD message suppression, use the `ipv6 mld snooping listener-message-suppression` global configuration command.

### Displaying MLD Snooping Information

You can display MLD snooping information for dynamically learned and statically configured router ports and VLAN interfaces. You can also display MAC address multicast entries for a VLAN configured for MLD snooping.

To display MLD snooping information, use one or more of the privileged EXEC commands in Table 38-2.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ipv6 mld snooping</code> [vlan <code>vlan-id</code>]</td>
<td>Display the MLD snooping configuration information for all VLANs on the switch or for a specified VLAN. (Optional) Enter <code>vlan vlan-id</code> to display information for a single VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094.</td>
</tr>
<tr>
<td><code>show ipv6 mld snooping mrouter</code> [vlan <code>vlan-id</code>]</td>
<td>Display information on dynamically learned and manually configured multicast router interfaces. When you enable MLD snooping, the switch automatically learns the interface to which a multicast router is connected. These are dynamically learned interfaces. (Optional) Enter <code>vlan vlan-id</code> to display information for a single VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094.</td>
</tr>
<tr>
<td><code>show ipv6 mld snooping querier</code> [vlan <code>vlan-id</code>]</td>
<td>Display information about the IPv6 address and incoming port for the most-recently received MLD query messages in the VLAN. (Optional) Enter <code>vlan vlan-id</code> to display information for a single VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094.</td>
</tr>
</tbody>
</table>
### Displaying MLD Snooping Information

#### Table 38-2  Commands for Displaying MLD Snooping Information (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| `show ipv6 mld snooping multicast-address [vlan vlan-id] [count | dynamic | user]` | Display all IPv6 multicast address information or specific IPv6 multicast address information for the switch or a VLAN.  
- Enter `count` to show the group count on the switch or in a VLAN.  
- Enter `dynamic` to display MLD snooping learned group information for the switch or for a VLAN.  
- Enter `user` to display MLD snooping user-configured group information for the switch or for a VLAN. |
| `show ipv6 mld snooping multicast-address vlan vlan-id [ipv6-multicast-address]` | Display MLD snooping for the specified VLAN and IPv6 multicast address. |
CHAPTER 39

Configuring IPv6 ACLs

This chapter includes information about configuring IPv6 ACLs on the Catalyst 3750 Metro switch. You can filter IP version 6 (IPv6) traffic by creating IPv6 access control lists (ACLs) and applying them to interfaces similarly to the way that you create and apply IP version 4 (IPv4) named ACLs. You can also create and apply input router ACLs to filter Layer 3 management traffic.

Note
To use IPv6, you must configure the dual IPv4 and IPv6 Switch Database Management (SDM) template on the switch. You select the template by entering the `sdm prefer dual-ipv4-and-ipv6` global configuration command.

For related information, see these chapters:
- For more information about SDM templates, see Chapter 6, “Configuring SDM Templates.”
- For information about IPv6 on the switch, see Chapter 37, “Configuring IPv6 Unicast Routing.”
- For information about ACLs on the switch, see Chapter 39, “Configuring IPv6 ACLs.”

Note
For complete syntax and usage information for the commands used in this chapter, see the command reference for this release or the Cisco IOS documentation referenced in the procedures.

This chapter contains these sections:
- Understanding IPv6 ACLs, page 39-1
- Configuring IPv6 ACLs, page 39-3
- Displaying IPv6 ACLs, page 39-8

Understanding IPv6 ACLs

The switch supports two types of IPv6 ACLs:
- IPv6 router ACLs
  - Supported on outbound or inbound traffic on Layer 3 interfaces, which can be routed ports, switch virtual interfaces (SVIs), or Layer 3 EtherChannels.
  - Applied to only IPv6 packets that are routed.
Chapter 39      Configuring IPv6 ACLs

Understanding IPv6 ACLs

- IPv6 port ACLs
  - Supported on inbound traffic on Layer 2 interfaces only.
  - Applied to all IPv6 packets entering the interface.

The switch supports only input port ACLs.

Note

If you configure unsupported IPv6 ACLs, an error message appears and the configuration does not take affect.

The switch does not support VLAN ACLs (VLAN maps) for IPv6 traffic.

Note

For more information about ACL support on the switch, see Chapter 33, “Configuring Network Security with ACLs.”

You can apply both IPv4 and IPv6 ACLs to an interface.

As with IPv4 ACLs, IPv6 port ACLs take precedence over router ACLs:

- When an input router ACL and input port ACL exist in an SVI, packets received on ports to which a port ACL is applied are filtered by the port ACL. Routed IP packets received on other ports are filtered by the router ACL. Other packets are not filtered.

- When an output router ACL and input port ACL exist in an SVI, packets received on the ports to which a port ACL is applied are filtered by the port ACL. Outgoing routed IPv6 packets are filtered by the router ACL. Other packets are not filtered.

Note

If any port ACL (IPv4, IPv6, or MAC) is applied to an interface, that port ACL is used to filter packets, and any router ACLs attached to the SVI of the port VLAN are ignored.

These sections describe some characteristics of IPv6 ACLs on the switch:

- Supported ACL Features, page 39-2
- IPv6 ACL Limitations, page 39-3

Supported ACL Features

IPv6 ACLs on the switch have these characteristics:

- Fragmented frames (the fragments keyword as in IPv4) are supported.
- The same statistics supported in IPv4 are supported for IPv6 ACLs.
- If the switch runs out of TCAM space, packets associated with the ACL label are forwarded to the CPU, and the ACLs are applied in software.
- Routed or bridged packets with hop-by-hop options have IPv6 ACLs applied in software.
- Logging is supported for router ACLs, but not for port ACLs.
IPv6 ACL Limitations

With IPv4, you can configure standard and extended numbered IP ACLs, named IP ACLs, and MAC ACLs. IPv6 supports only named ACLs.

The switch supports most Cisco IOS-supported IPv6 ACLs with some exceptions:

- IPv6 source and destination addresses—ACL matching is supported only on prefixes from /0 to /64 and host addresses (/128) that are in the extended universal identifier (EUI)-64 format. The switch supports only these host addresses with no loss of information:
  - aggregatable global unicast addresses
  - link local addresses
- The switch does not support matching on these keywords: \texttt{flowlabel}, \texttt{routing header}, and \texttt{undetermined-transport}.
- The switch does not support reflexive ACLs (the \texttt{reflect} keyword).
- This release supports only port ACLs and router ACLs for IPv6; it does not support VLAN ACLs (VLAN maps).
- The switch does not apply MAC-based ACLs on IPv6 frames.
- You cannot apply IPv6 port ACLs to Layer 2 EtherChannels.
- The switch does not support output port ACLs.
- When configuring an ACL, there is no restriction on keywords entered in the ACL, regardless of whether or not they are supported on the platform. When you apply the ACL to an interface that requires hardware forwarding (physical ports or SVIs), the switch checks to determine whether or not the ACL can be supported on the interface. If not, attaching the ACL is rejected.
- If an ACL is applied to an interface and you attempt to add an access control entry (ACE) with an unsupported keyword, the switch does not allow the ACE to be added to the ACL that is currently attached to the interface.

Configuring IPv6 ACLs

Before configuring IPv6 ACLs, you must select one of the dual IPv4 and IPv6 SDM templates. To filter IPv6 traffic, you perform these steps:

\begin{itemize}
  \item \textbf{Step 1} Create an IPv6 ACL, and enter IPv6 access list configuration mode.
  \item \textbf{Step 2} Configure the IPv6 ACL to block (deny) or pass (permit) traffic.
  \item \textbf{Step 3} Apply the IPv6 ACL to an interface. For router ACLs, you must also configure an IPv6 address on the Layer 3 interface to which the ACL is applied.
\end{itemize}

These sections describe how to configure and apply IPv6 ACLs:

- Default IPv6 ACL Configuration, page 39-4
- Interaction with Other Features, page 39-4
- Creating IPv6 ACLs, page 39-4
- Applying an IPv6 ACL to an Interface, page 39-7
Default IPv6 ACL Configuration

There are no IPv6 ACLs configured or applied.

Interaction with Other Features

Configuring IPv6 ACLs has these interactions with other features or switch characteristics:

- If an IPv6 router ACL is configured to deny a packet, the packet is dropped. A copy of the packet is sent to the Internet Control Message Protocol (ICMP) queue to generate an ICMP unreachable message for the frame.
- If a bridged frame is to be dropped due to a port ACL, the frame is not bridged.
- You can create both IPv4 and IPv6 ACLs on a switch, and you can apply both IPv4 and IPv6 ACLs to the same interface. Each ACL must have a unique name; an error message appears if you try to use a name that is already configured.
- You use different commands to create IPv4 and IPv6 ACLs and to attach IPv4 or IPv6 ACLs to the same Layer 2 or Layer 3 interface. If you use the wrong command to attach an ACL (for example, an IPv4 command to attach an IPv6 ACL), you receive an error message.
- You cannot use MAC ACLs to filter IPv6 frames. MAC ACLs can only filter non-IP frames.
- If the TCAM is full, for any additional configured ACLs, packets are forwarded to the CPU, and the ACLs are applied in software.

Creating IPv6 ACLs

Beginning in privileged EXEC mode, follow these steps to create an IPv6 ACL:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td></td>
</tr>
<tr>
<td>ipv6 access-list access-list-name</td>
<td>Define an IPv6 access list name, and enter IPv6 access-list configuration mode.</td>
</tr>
</tbody>
</table>
Step 3a

deny | permit protocol
(source-ipv6-prefix|prefix-length | any | host source-ipv6-address)
[operator [port-number]]
(destination-ipv6-prefix/
prefix-length | any | host destination-ipv6-address)
[operator [port-number]]
[dscp value] [fragments] [log]
[log-input] [sequence value]
[time-range name]

Purpose

Enter deny or permit to specify whether to deny or permit the packet if conditions are matched. These are the conditions:

- For protocol, enter the name or number of an Internet protocol: ahp, esp, icmp, ipv6, pcp, stcp, tcp, or udp, or an integer in the range 0 to 255 representing an IPv6 protocol number. For additional specific parameters for ICMP, TCP, and UDP, see Steps 3b through 3d.

- The source-ipv6-prefix|prefix-length or destination-ipv6-prefix|prefix-length is the source or destination IPv6 network or class of networks for which to set deny or permit conditions, specified in hexadecimal and using 16-bit values between colons (see RFC 2373).

Note

Although the CLI help shows a prefix-length range of /0 to /128, the switch supports IPv6 address matching only for prefixes in the range of /0 to /64 and EUI-based /128 prefixes for aggregatable global unicast and link-local host addresses.

- Enter any as an abbreviation for the IPv6 prefix ::/0.

- For host source-ipv6-address or destination-ipv6-address, enter the source or destination IPv6 host address for which to set deny or permit conditions, specified in hexadecimal using 16-bit values between colons.

- (Optional) For operator, specify an operand that compares the source or destination ports of the specified protocol. Operands are lt (less than), gt (greater than), eq (equal), neq (not equal), and range.

If the operator follows the source-ipv6-prefix|prefix-length argument, it must match the source port. If the operator follows the destination-ipv6-prefix|prefix-length argument, it must match the destination port.

- (Optional) The port-number is a decimal number from 0 to 65535 or the name of a TCP or UDP port for filtering TCP or UDP, respectively.

- (Optional) Enter dscp value to match a differentiated services code point value against the traffic class value in the Traffic Class field of each IPv6 packet header. The acceptable range is from 0 to 63.

- (Optional) Enter fragments to check noninitial fragments. This keyword is visible only if the protocol is ipv6.

- (Optional) Enter log to cause an logging message to be sent to the console about the packet that matches the entry. Enter log-input to include the input interface in the log entry. Logging is supported only for router ACLs.

- (Optional) Enter sequence value to specify the sequence number for the access list statement. The acceptable range is from 1 to 4294967295.

- (Optional) Enter time-range name to specify a time range for the statement.
### Chapter 39 Configuring IPv6 ACLs

#### Command

<table>
<thead>
<tr>
<th>Step 3b</th>
<th>deny</th>
<th>permit tcp</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>{source-ipv6-prefix</td>
<td>prefix-length</td>
</tr>
<tr>
<td></td>
<td>[operator [port-number]]</td>
<td>[ack]</td>
</tr>
</tbody>
</table>

(Optional) Define a TCP access list and the access conditions.

Enter **tcp** for Transmission Control Protocol. The parameters are the same as those described in Step 3a, with these additional optional parameters:

- **ack**—Acknowledgment bit set.
- **established**—An established connection. A match occurs if the TCP datagram has the ACK or RST bits set.
- **fin**—Finished bit set; no more data from sender.
- **neq** {port | protocol}—Matches only packets that are not on a given port number.
- **psh**—Push function bit set.
- **range** {port | protocol}—Matches only packets in the port number range.
- **rst**—Reset bit set.
- **syn**—Synchronize bit set.
- **urg**—Urgent pointer bit set.

<table>
<thead>
<tr>
<th>Step 3c</th>
<th>deny</th>
<th>permit udp</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>{source-ipv6-prefix</td>
<td>prefix-length</td>
</tr>
<tr>
<td></td>
<td>[operator [port-number]]</td>
<td>[dscp value]</td>
</tr>
</tbody>
</table>

(Optional) Define a UDP access list and the access conditions.

Enter **udp** for the User Datagram Protocol. The UDP parameters are the same as those described for TCP, except that the [operator [port]] port number or name must be a UDP port number or name, and the **established** parameter is not valid for UDP.

<table>
<thead>
<tr>
<th>Step 3d</th>
<th>deny</th>
<th>permit icmp</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>{source-ipv6-prefix</td>
<td>prefix-length</td>
</tr>
<tr>
<td></td>
<td>[operator [port-number]]</td>
<td>[icmp-type</td>
</tr>
</tbody>
</table>

(Optional) Define an ICMP access list and the access conditions.

Enter **icmp** for Internet Control Message Protocol. The ICMP parameters are the same as those described for most IP protocols in Step 3a, with the addition of the ICMP message type and code parameters. These optional keywords have these meanings:

- **icmp-type**—Enter to filter by ICMP message type, a number from 0 to 255.
- **icmp-code**—Enter to filter ICMP packets that are filtered by the ICMP message code type, a number from 0 to 255.
- **icmp-message**—Enter to filter ICMP packets by the ICMP message type name or the ICMP message type and code name. To see a list of ICMP message type names and code names, use the ? key or see command reference for this release.

<table>
<thead>
<tr>
<th>Step 4</th>
<th>end</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>show ipv6 access-list</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Verify the access list configuration.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>copy running-config startup-config</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
Use the **no deny | permit** IPv6 access-list configuration commands with keywords to remove the deny or permit conditions from the specified access list.

This example configures the IPv6 access list named CISCO. The first deny entry in the list denies all packets that have a destination TCP port number greater than 5000. The second deny entry denies packets that have a source UDP port number less than 5000. The second deny also logs all matches to the console. The first permit entry in the list permits all ICMP packets. The second permit entry in the list permits all other traffic. The second permit entry is necessary because an implicit deny -all condition is at the end of each IPv6 access list.

```plaintext
Switch(config)# ipv6 access-list CISCO
Switch(config-ipv6-acl)# deny tcp any any gt 5000
Switch(config-ipv6-acl)# deny ::/0 lt 5000 ::/0 log
Switch(config-ipv6-acl)# permit icmp any any
Switch(config-ipv6-acl)# permit any any
```

### Applying an IPv6 ACL to an Interface

This section describes how to apply IPv6 ACLs to network interfaces. You can apply an ACL to outbound or inbound traffic on Layer 3 interfaces, or to inbound traffic on Layer 2 interfaces.

Beginning in privileged EXEC mode, follow these steps to control access to an interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>interface interface-id</td>
<td>Identify a Layer 2 interface (for port ACLs) or Layer 3 interface (for router ACLs) on which to apply an access list, and enter interface configuration mode.</td>
</tr>
<tr>
<td>3</td>
<td>no switchport</td>
<td>If applying a router ACL, change the interface from Layer 2 mode (the default) to Layer 3 mode.</td>
</tr>
<tr>
<td>4</td>
<td>ipv6 address ipv6-address</td>
<td>Configure an IPv6 address on a Layer 3 interface (for router ACLs). This command is not required on Layer 2 interfaces or if the interface has already been configured with an explicit IPv6 address.</td>
</tr>
<tr>
<td></td>
<td>ipv6 traffic-filter access-list-name {in</td>
<td>out}</td>
</tr>
<tr>
<td>6</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>7</td>
<td>show running-config</td>
<td>Verify the access list configuration.</td>
</tr>
<tr>
<td>8</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Use the **no ipv6 traffic-filter access-list-name** interface configuration command to remove an access list from an interface.

This example shows how to apply the access list CISCO to outbound traffic on a Layer 3 interface:

```plaintext
Switch(config)# interface gigabitethernet1/1/1
Switch(config-if)# no switchport
Switch(config-if)# ipv6 address 2001::/64 eui-64
Switch(config-if)# ipv6 traffic-filter CISCO out
```
Displaying IPv6 ACLs

You can display information about all configured access lists, all IPv6 access lists, or a specific access list by using one or more of the privileged EXEC commands in Table 39-1.

Table 39-1 Commands for Displaying IPv6 Access List Information

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show access-lists</td>
<td>Display all access lists configured on the switch.</td>
</tr>
<tr>
<td>show ipv6 access-list [access-list-name]</td>
<td>Display all configured IPv6 access list or the access list specified by name.</td>
</tr>
</tbody>
</table>

This is an example of the output from the **show access-lists** privileged EXEC command. The output shows all access lists that are configured on the switch.

```
Switch #show access-lists
Extended IP access list hello
10 permit ip any any
IPv6 access list ipv6
   permit ipv6 any any sequence 10
```

This is an example of the output from the **show ipv6 access-lists** privileged EXEC command. The output shows only IPv6 access lists configured on the switch.

```
Switch# show ipv6 access-list
IPv6 access list inbound
   permit tcp any any eq bgp (8 matches) sequence 10
   permit tcp any any eq telnet (15 matches) sequence 20
   permit udp any any sequence 30
IPv6 access list outbound
   deny udp any any sequence 10
   deny tcp any any eq telnet sequence 20
```
CHAPTER 40

Configuring HSRP

This chapter describes how to use Hot Standby Router Protocol (HSRP) on the Catalyst 3750 Metro switch to provide routing redundancy for routing IP traffic without being dependent on the availability of any single router.

For complete syntax and usage information for the commands used in this chapter, see the switch command reference for this release and the *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2*.

This chapter consists of these sections:

- Understanding HSRP, page 40-1
- Configuring HSRP, page 40-4
- Displaying HSRP Configurations, page 40-10

Understanding HSRP

HSRP is Cisco’s standard method of providing high network availability by providing first-hop redundancy for IP hosts on an IEEE 802 LAN configured with a default gateway IP address. HSRP routes IP traffic without relying on the availability of any single router. It enables a set of router interfaces to work together to present the appearance of a single virtual router or default gateway to the hosts on a LAN. When HSRP is configured on a network or segment, it provides a virtual Media Access Control (MAC) address and an IP address that is shared among a group of configured routers. HSRP allows two or more HSRP-configured routers to use the MAC address and IP network address of a virtual router. The virtual router does not exist; it represents the common target for routers that are configured to provide backup to each other. One of the routers is selected to be the active router and another to be the standby router, which assumes control of the group MAC address and IP address should the designated active router fail.

Note

Routers in an HSRP group can be any router interface that supports HSRP, including Catalyst 3750 Metro switch routed ports and switch virtual interfaces (SVIs).
HSRP provides high network availability by providing redundancy for IP traffic from hosts on networks. In a group of router interfaces, the active router is the router of choice for routing packets; the standby router is the router that takes over the routing duties when an active router fails or when preset conditions are met.

HSRP is useful for hosts that do not support a router discovery protocol and cannot switch to a new router when their selected router reloads or loses power. When HSRP is configured on a network segment, it provides a virtual MAC address and an IP address that is shared among router interfaces in a group of router interfaces running HSRP. The router selected by the protocol to be the active router receives and routes packets destined for the group’s MAC address. For \( n \) routers running HSRP, there are \( n + 1 \) IP and MAC addresses assigned.

HSRP detects when the designated active router fails, and a selected standby router assumes control of the Hot Standby group’s MAC and IP addresses. A new standby router is also selected at that time. Devices running HSRP send and receive multicast UDP-based hello packets to detect router failure and to designate active and standby routers. When HSRP is configured on an interface, Internet Control Message Protocol (ICMP) redirect messages are automatically enabled for the interface.

You can configure multiple Hot Standby groups among switches that are operating in Layer 3 to make more use of the redundant routers. To do so, specify a group number for each Hot Standby command group you configure for an interface. For example, you might configure an interface on switch 1 as an active router and one on switch 2 as a standby router and also configure another interface on switch 2 as an active router with another interface on switch 1 as its standby router.

Figure 40-1 shows a segment of a network configured for HSRP. Each router is configured with the MAC address and IP network address of the virtual router. Instead of configuring hosts on the network with the IP address of Router A, you configure them with the IP address of the virtual router as their default router. When Host C sends packets to Host B, it sends them to the MAC address of the virtual router. If for any reason, Router A stops transferring packets, Router B responds to the virtual IP address and virtual MAC address and becomes the active router, assuming the active router duties. Host C continues to use the IP address of the virtual router to address packets destined for Host B, which Router B now receives and sends to Host B. Until Router A resumes operation, HSRP allows Router B to provide uninterrupted service to users on Host C’s segment that need to communicate with users on Host B’s segment and also continues to perform its normal function of handling packets between the Host A segment and Host B.
HSRP Versions

Cisco IOS Release 12.2(46)SE and later support these Hot Standby Router Protocol (HSRP) versions:

- **HSRPv1**—Version 1 of the HSRP, the default version of HSRP. It has these features:
  - The HSRP group number can be from 0 to 255.
  - HSRPv1 uses the multicast address 224.0.0.2 to send hello packets, which can conflict with Cisco Group Management Protocol (CGMP) leave processing. You cannot enable HSRPv1 and CGMP at the same time; they are mutually exclusive.

- **HSRPv2**—Version 2 of the HSRP has these features:
  - To match the HSRP group number to the VLAN ID of a subinterface, HSRPv2 can use a group number from 0 to 4095 and a MAC address from 0000.0C9F.F000 to 0000.0C9F.FFFF.
  - HSRPv2 uses the multicast address 224.0.0.102 to send hello packets. HSRPv2 and CGMP leave processing are no longer mutually exclusive, and both can be enabled at the same time.
  - HSRPv2 has a different packet format than HSRPv1.

A switch running HSRPv1 cannot identify the physical router that sent a hello packet because the source MAC address of the router is the virtual MAC address.
Configuring HSRP

These sections include HSRP configuration information:
- Default HSRP Configuration, page 40-4
- HSRP Configuration Guidelines, page 40-4
- Enabling HSRP, page 40-5
- Configuring HSRP Group Attributes, page 40-6
- Enabling HSRP Support for ICMP Redirect Messages, page 40-10

Default HSRP Configuration

Table 40-1 shows the default HSRP configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>HSRP version</td>
<td>Version 1</td>
</tr>
<tr>
<td>HSRP groups</td>
<td>None configured</td>
</tr>
<tr>
<td>Standby group number</td>
<td>0</td>
</tr>
<tr>
<td>Standby MAC address</td>
<td>System assigned as: 0000.0c07.acXX, where XX is the HSRP group number</td>
</tr>
<tr>
<td>Standby priority</td>
<td>100</td>
</tr>
<tr>
<td>Standby delay</td>
<td>0 (no delay)</td>
</tr>
<tr>
<td>Standby track interface priority</td>
<td>10</td>
</tr>
<tr>
<td>Standby hello time</td>
<td>3 seconds</td>
</tr>
<tr>
<td>Standby holdtime</td>
<td>10 seconds</td>
</tr>
</tbody>
</table>

HSRP Configuration Guidelines

Follow these guidelines when configuring HSRP:
- HSRP can be configured on a maximum of 32 VLAN or routing interfaces.
- In the following procedures, the specified interface must be one of these Layer 3 interfaces:
  - Routed port: a physical port configured as a Layer 3 port by entering the no switchport interface configuration command.
- SVI: a VLAN interface created by using the `interface vlan vlan_id` global configuration command and by default a Layer 3 interface.

- Etherchannel port channel in Layer 3 mode: a port-channel logical interface created by using the `interface port-channel port-channel-number` global configuration command and binding the Ethernet interface into the channel group. For more information, see the “Configuring Layer 3 EtherChannels” section on page 35-13.

- All Layer 3 interfaces must have IP addresses assigned to them. See the “Configuring Layer 3 Interfaces” section on page 9-17.

- HSRPv2 and HSRPv1 can be configured on the same switch if HSRPv2 is configured on different interfaces than those on which HSRPv1 is configured.

- The version of an HSRP group can be changed from HSRPv2 to HSRPv1 only if the group number is less than 256.

- If you change the HSRP version on an interface, each HSRP group resets because it now has a new virtual MAC address.

### Enabling HSRP

The `standby ip` interface configuration command activates HSRP on the configured interface. If an IP address is specified, that address is used as the designated address for the Hot Standby group. If no IP address is specified, the address is learned through the standby function. You must configure at least one Layer 3 port on the LAN with the designated address. Configuring an IP address always overrides another designated address currently in use.

When the `standby ip` command is enabled on an interface and proxy ARP is enabled, if the interface’s Hot Standby state is active, proxy ARP requests are answered using the Hot Standby group MAC address. If the interface is in a different state, proxy ARP responses are suppressed.

**Note**

When multi-VRF CE is configured, you cannot assign the same HSRP standby address to two different VPNs.

Beginning in privileged EXEC mode, follow these steps to create or enable HSRP on a Layer 3 interface:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
<td>Enter interface configuration mode, and enter the Layer 3 interface on which you want to enable HSRP.</td>
</tr>
<tr>
<td>Step 3</td>
<td>standby version {1</td>
<td>2}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1— Select HSRPv1.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 2— Select HSRPv2.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you do not enter this command or do not specify a keyword, the interface runs the default HSRP version, HSRP v1.</td>
</tr>
</tbody>
</table>
Configuring HSRP

Use the `no standby [group-number] ip [ip-address [secondary]]` interface configuration command to disable HSRP.

This example shows how to activate HSRP for group 1 on an interface. The IP address used by the hot standby group is learned by using HSRP.

### Note

This procedure is the minimum number of steps required to enable HSRP.

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# standby 1 ip
Switch(config-if)# end
Switch# show standby
```

### Configuring HSRP Group Attributes

Although HSRP can run with no other configuration required, you can configure attributes for the HSRP group, including authentication, priority, preemption and preemption delay, timers, or MAC address.

### Configuring HSRP Priority

The `standby priority`, `standby preempt`, and `standby track` interface configuration commands are all used to set characteristics for determining active and standby routers and behavior regarding when a new active router takes over. When configuring priority, follow these guidelines:

- Assigning a priority allows you to select the active and standby routers. If preemption is enabled, the router with the highest priority becomes the active router. If priorities are equal, the current active router does not change.
- The highest number (1 to 255) represents the highest priority (most likely to become the active router).
- When setting the priority, preempt, or both, you must specify at least one keyword (priority, preempt, or both).
- The priority of the device can change dynamically if an interface is configured with the `standby track` command and another interface on the router goes down.
- The `standby track` interface configuration command ties the router hot standby priority to the availability of its interfaces and is useful for tracking interfaces that are not configured for HSRP. When a tracked interface fails, the hot standby priority on the device on which tracking has been configured decreases by 10. If an interface is not tracked, its state changes do not affect the hot standby priority of the configured device. For each interface configured for hot standby, you can configure a separate list of interfaces to be tracked.
- The `standby track interface-priority` interface configuration command specifies how much to decrement the hot standby priority when a tracked interface goes down. When the interface comes back up, the priority is incremented by the same amount.
- When multiple tracked interfaces are down and `interface-priority` values have been configured, the configured priority decrements are cumulative. If tracked interfaces that were not configured with priority values fail, the default decrement is 10, and it is noncumulative.
- When routing is first enabled for the interface, it does not have a complete routing table. If it is configured to preempt, it becomes the active router, even though it is unable to provide adequate routing services. To solve this problem, configure a delay time to allow the router to update its routing table.

Beginning in privileged EXEC mode, use one or more of these steps to configure HSRP priority characteristics on an interface:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>interface interface-id</strong></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>standby [group-number] priority priority</strong></td>
</tr>
<tr>
<td></td>
<td>- (Optional) <code>group-number</code>—The group number to which the command applies.</td>
</tr>
</tbody>
</table>
### Step 4

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>standby [group-number] preempt [delay minimum seconds] [reload seconds] [sync seconds]]</td>
<td>Configure the router to preempt, which means that when the local router has a higher priority than the active router, it becomes the active router.</td>
</tr>
<tr>
<td>- (Optional) group-number — The group number to which the command applies.</td>
<td></td>
</tr>
<tr>
<td>- (Optional) delay minimum — Set to cause the local router to postpone taking over the active role for the number of seconds shown. The range is 0 to 36000 seconds (1 hour); the default is 0 (no delay before taking over).</td>
<td></td>
</tr>
<tr>
<td>- (Optional) delay reload — Set to cause the local router to postpone taking over the active role after a reload for the number of seconds shown. The range is 0 to 36000 seconds (1 hour); the default is 0 (no delay before taking over after a reload).</td>
<td></td>
</tr>
<tr>
<td>- (Optional) delay sync — Set to cause the local router to postpone taking over the active role so that IP redundancy clients can reply (either with an ok or wait reply) for the number of seconds shown. The range is 0 to 36000 seconds (1 hour); the default is 0 (no delay before taking over).</td>
<td></td>
</tr>
<tr>
<td>Use the no form of the command to restore the default values.</td>
<td></td>
</tr>
</tbody>
</table>

### Step 5

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>standby [group-number] track type number [interface-priority]</td>
<td>Configure an interface to track other interfaces so that if one of the other interfaces goes down, the device’s Hot Standby priority is lowered.</td>
</tr>
<tr>
<td>- (Optional) group-number — The group number to which the command applies.</td>
<td></td>
</tr>
<tr>
<td>- type — Enter the interface type (combined with interface number) that is tracked.</td>
<td></td>
</tr>
<tr>
<td>- number — Enter the interface number (combined with interface type) that is tracked.</td>
<td></td>
</tr>
<tr>
<td>- (Optional) interface-priority — Enter the amount by which the hot standby priority for the router is decremented or incremented when the interface goes down or comes back up. The default value is 10.</td>
<td></td>
</tr>
</tbody>
</table>

### Step 6

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

### Step 7

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show running-config</td>
<td>Verify the configuration of the standby groups.</td>
</tr>
</tbody>
</table>

### Step 8

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Use the no standby [group-number] priority priority [preempt delay delay] and no standby [group-number] [priority priority] preempt [delay delay] interface configuration commands to restore default priority, preempt, and delay values.

Use the no standby [group-number] track type number [interface-priority] interface configuration command to remove the tracking.

This example activates a port, sets an IP address and a priority of 120 (higher than the default value), and waits for 300 seconds (5 minutes) before attempting to become the active router:

```bash
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# standby ip 172.19.108.254
Switch(config-if)# standby priority 120 preempt delay 300
Switch(config-if)# end
Switch# ```
Configuring HSRP Authentication and Timers

You can optionally configure an HSRP authentication string or change the hello-time interval and holdtime.

When configuring these attributes, follow these guidelines:

- The authentication string is sent unencrypted in all HSRP messages. You must configure the same authentication string on all routers and access servers on a cable to ensure interoperation. Authentication mismatch prevents a device from learning the designated Hot Standby IP address and timer values from other routers configured with HSRP.

- Routers or access servers on which standby timer values are not configured can learn timer values from the active or standby router. The timers configured on an active router always override any other timer settings.

- All routers in a Hot Standby group should use the same timer values. Normally, the holdtime is greater than or equal to 3 times the hello-time.

Beginning in privileged EXEC mode, use one or more of these steps to configure HSRP authentication and timers on an interface:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Enter interface configuration mode, and enter the HSRP interface on which you want to set authentication.</td>
</tr>
<tr>
<td>Step 3 standby [group-number] authentication string</td>
<td>(Optional) <strong>authentication string</strong>—Enter a string to be carried in all HSRP messages. The authentication string can be up to eight characters in length; the default string is cisco. (Optional) <strong>group-number</strong>—The group number to which the command applies.</td>
</tr>
</tbody>
</table>
| Step 4 standby [group-number] timers hello-time holdtime | (Optional) Configure the time between hello packets and the time before other routers declare the active router to be down. 
  - **group-number**—The group number to which the command applies. 
  - **hello-time**—The hello interval in seconds. The range is from 1 to 255; the default is 3 seconds. 
  - **holdtime**—The time in seconds before the active or standby router is declared to be down. The range is from 1 to 255; the default is 10 seconds. |
| Step 5 end                   | Return to privileged EXEC mode.                                 |
| Step 6 show running-config   | Verify the configuration of the standby groups.                |
| Step 7 copy running-config startup-config | (Optional) Save your entries in the configuration file. |

Use the **no standby [group-number] authentication string** interface configuration command to delete an authentication string. Use the **no standby [group-number] timers hello-time holdtime** interface configuration command to restore timers to their default values.
This example shows how to configure *word* as the authentication string required to allow Hot Standby routers in group 1 to interoperate:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# standby 1 authentication word
Switch(config-if)# end
Switch#
```

This example shows how to set the timers on standby group 1 with the time between hello packets at 5 seconds and the time after which a router is considered down to be 15 seconds:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# standby 1 ip
Switch(config-if)# standby 1 timers 5 15
Switch(config-if)# end
Switch#
```

### Enabling HSRP Support for ICMP Redirect Messages

ICMP (Internet Control Message Protocol) redirect messages are automatically enabled on interfaces configured with HSRP. This feature filters outgoing ICMP redirect messages through HSRP, in which the next hop IP address might be changed to an HSRP virtual IP address. ICMP is a network layer Internet protocol that provides message packets to report errors and other information relevant to IP processing. ICMP provides diagnostic functions, such as sending and directing error packets to the host.

When the switch is running HSRP, make sure hosts do not discover the interface (or real) MAC addresses of routers in the HSRP group. If a host is redirected by ICMP to the real MAC address of a router and that router later fails, packets from the host are lost.

For more information, see the *Cisco IOS IP Configuration Guide, Release 12.2*.

### Displaying HSRP Configurations

From privileged EXEC mode, use this command to display HSRP settings:

```
show standby [interface-id [group]] [brief] [detail]
```

You can display HSRP information for the whole switch, for a specific interface, for an HSRP group, or for an HSRP group on an interface. You can also specify whether to display a concise overview of HSRP information or detailed HSRP information. The default display is *detail*. If there are a large number of HSRP groups, using the `show standby` command without qualifiers can result in an unwieldy display.

This is an example of output from the `show standby` privileged EXEC command, displaying HSRP information for two standby groups (group 1 and group 100):

```
Switch# show standby
VLAN1 - Group 1
  Local state is Standby, priority 105, may preempt
  Hellotime 3 holdtime 10
  Next hello sent in 00:00:02.182
  Hot standby IP address is 10.0.0.1 configured
  Active router is 172.20.138.35 expires in 00:00:09
  Standby router is local
  Standby virtual mac address is 0000.0c07.ac01
  Name is bbb
```
VLAN1 - Group 100
Local state is Active, priority 105, may preempt
Hello-time 3 holdtime 10
Next hello sent in 00:00:02.262
Hot standby IP address is 172.20.138.51 configured
Active router is local
Standby router is unknown expired
Standby virtual mac address is 0000.0c07.ac64
Name is test
Configuring Cisco IOS IP SLAs Operations

This chapter describes how to use Cisco IOS IP Service Level Agreements (SLAs) and the IETF Two-Way Active Measurement Protocol (TWAMP) on the Catalyst 3750 Metro switch. Cisco IP SLAs is a part of Cisco IOS software that allows Cisco customers to analyze IP service levels for IP applications and services by using active traffic monitoring—the generation of traffic in a continuous, reliable, and predictable manner—for measuring network performance. With Cisco IOS IP SLAs, service provider customers can measure and provide service level agreements, and enterprise customers can verify service levels, verify outsourced service level agreements, and understand network performance. Cisco IOS IP SLAs can perform network assessments, verify quality of service (QoS), ease the deployment of new services, and assist with network troubleshooting.

TWAMP defines a standard for measuring round-trip network traffic between any two devices that support the protocol. Beginning with Cisco IOS Release 12.2(52)SE, you can implement TWAMP on Catalyst 3750 Metro switches.

For more information about IP SLAs, see the Cisco IOS IP SLAs Configuration Guide, Release 12.4T at this URL:


For command syntax information, see the command reference at this URL:


This chapter consists of these sections:

- Understanding Cisco IOS IP SLAs, page 41-1
- Configuring IP SLAs Operations, page 41-6
- Monitoring IP SLAs Operations, page 41-13
- Understanding TWAMP, page 41-14
- Configuring TWAMP, page 41-15

Understanding Cisco IOS IP SLAs

Cisco IOS IP SLAs sends data across the network to measure performance between multiple network locations or across multiple network paths. It simulates network data and IP services and collects network performance information in real time. Cisco IOS IP SLAs generates and analyzes traffic either between Cisco IOS devices or from a Cisco IOS device to a remote IP device such as a network application server. Measurements provided by the various Cisco IOS IP SLAs operations can be used for troubleshooting, for problem analysis, and for designing network topologies.
Depending on the specific Cisco IOS IP SLAs operation, various network performance statistics are monitored within the Cisco device and stored in both command-line interface (CLI) and Simple Network Management Protocol (SNMP) MIBs. IP SLAs packets have configurable IP and application layer options such as source and destination IP address, User Datagram Protocol (UDP)/TCP port numbers, a type of service (ToS) byte (including Differentiated Services Code Point [DSCP] and IP Prefix bits), Virtual Private Network (VPN) routing/forwarding instance (VRF), and URL web address.

Because Cisco IP SLAs is Layer 2 transport independent, you can configure end-to-end operations over disparate networks to best reflect the metrics that an end user is likely to experience. IP SLAs collects a unique subset of these performance metrics:

- Delay (both round-trip and one-way)
- Jitter (directional)
- Packet loss (directional)
- Packet sequencing (packet ordering)
- Path (per hop)
- Connectivity (directional)
- Server or website download time

Because Cisco IOS IP SLAs is SNMP-accessible, it can also be used by performance-monitoring applications like CiscoWorks Internetwork Performance Monitor (IPM) and other third-party Cisco partner performance management products. You can find more details about network management products that use Cisco IOS IP SLAs at this URL:

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

Using IP SLAs can provide these benefits:

- Service-level agreement monitoring, measurement, and verification.
- Network performance monitoring
  - Measures the jitter, latency, or packet loss in the network.
  - Provides continuous, reliable, and predictable measurements.
- IP service network health assessment to verify that the existing QoS is sufficient for new IP services.
- Edge-to-edge network availability monitoring for proactive verification and connectivity testing of network resources (for example, shows the network availability of an NFS server used to store business critical data from a remote site).
- Troubleshooting of network operation by providing consistent, reliable measurement that immediately identifies problems and saves troubleshooting time.
- Multiprotocol Label Switching (MPLS) performance monitoring and network verification (if the switch supports MPLS)

This section includes this information about IP SLAs functionality:

- Using Cisco IOS IP SLAs to Measure Network Performance, page 41-3
- IP SLAs Responder and IP SLAs Control Protocol, page 41-4
- Response Time Computation for IP SLAs, page 41-4
- IP SLAs Operation Scheduling, page 41-5
- IP SLAs Operation Threshold Monitoring, page 41-5
Using Cisco IOS IP SLAs to Measure Network Performance

You can use IP SLAs to monitor the performance between any area in the network—core, distribution, and edge—without deploying a physical probe. It uses generated traffic to measure network performance between two networking devices. Figure 41-1 shows how IP SLAs begins when the source device sends a generated packet to the destination device. After the destination device receives the packet, depending on the type of IP SLAs operation, it responds with time-stamp information for the source to make the calculation on performance metrics. An IP SLAs operation performs a network measurement from the source device to a destination in the network using a specific protocol such as UDP.

To implement IP SLAs network performance measurement, you need to perform these tasks:

1. Enable the IP SLAs responder, if required.
2. Configure the required IP SLAs operation type.
3. Configure any options available for the specified operation type.
4. Configure threshold conditions, if required.
5. Schedule the operation to run, then let the operation run for a period of time to gather statistics.
6. Display and interpret the results of the operation using the Cisco IOS CLI or a network management system (NMS) system with SNMP.

For more information about IP SLAs operations, see the operation-specific chapters in the Cisco IOS IP SLAs Configuration Guide at this URL:


Note

The switch does not support Voice over IP (VoIP) service levels using the gatekeeper registration delay operations measurements. Before configuring any IP SLAs application, you can use the show ip sla application privileged EXEC command to verify that the operation type is supported on your software image.
IP SLAs Responder and IP SLAs Control Protocol

The IP SLAs responder is a component embedded in the destination Cisco device that allows the system to anticipate and respond to IP SLAs request packets. The responder provides accurate measurements without the need for dedicated probes. The responder uses the Cisco IOS IP SLAs Control Protocol to provide a mechanism through which it can be notified on which port it should listen and respond. Only a Cisco IOS device can be a source for a destination IP SLAs Responder.

Note

The IP SLAs responder can be a Cisco IOS Layer 2, responder-configurable switch, such as a Catalyst 2960 or Cisco ME 2400 switch. The responder does not need to support full IP SLAs functionality.

Figure 41-1 shows where the Cisco IOS IP SLAs responder fits in the IP network. The responder listens on a specific port for control protocol messages sent by an IP SLAs operation. Upon receipt of the control message, it enables the specified UDP or TCP port for the specified duration. During this time, the responder accepts the requests and responds to them. It disables the port after it responds to the IP SLAs packet, or when the specified time expires. MD5 authentication for control messages is available for added security.

You do not need to enable the responder on the destination device for all IP SLAs operations. For example, a responder is not required for services that are already provided by the destination router (such as Telnet or HTTP). You cannot configure the IP SLAs responder on non-Cisco devices and Cisco IOS IP SLAs can send operational packets only to services native to those devices.

Response Time Computation for IP SLAs

Switches and routers can take tens of milliseconds to process incoming packets due to other high priority processes. This delay affects the response times because the test-packet reply might be in a queue while waiting to be processed. In this situation, the response times would not accurately represent true network delays. IP SLAs minimizes these processing delays on the source device as well as on the target device (if the responder is being used) to determine true round-trip times. IP SLAs test packets use time stamping to minimize the processing delays.

When the IP SLAs responder is enabled, it allows the target device to take time stamps when the packet arrives on the interface at interrupt level and again just as it is leaving, eliminating the processing time. This time stamping is made with a granularity of sub-milliseconds (ms).

Figure 41-2 demonstrates how the responder works. Four time stamps are taken to make the calculation for round-trip time. At the target router, with the responder functionality enabled, time stamp 2 (TS2) is subtracted from time stamp 3 (TS3) to produce the time spent processing the test packet as represented by delta. This delta value is then subtracted from the overall round-trip time. Notice that the same principle is applied by IP SLAs on the source router where the incoming time stamp 4 (TS4) is also taken at the interrupt level to allow for greater accuracy.
An additional benefit of the two time stamps at the target device is the ability to track one-way delay, jitter, and directional packet loss. Because much network behavior is asynchronous, it is critical to have these statistics. However, to capture one-way delay measurements, you must configure both the source router and target router with Network Time Protocol (NTP) so that the source and target are synchronized to the same clock source. One-way jitter measurements do not require clock synchronization.

**IP SLAs Operation Scheduling**

When you configure an IP SLAs operation, you must schedule the operation to begin capturing statistics and collecting error information. You can schedule an operation to start immediately or to start at a certain month, day, and hour. You can use the *pending* option to set the operation to start at a later time. The pending option is an internal state of the operation that is visible through SNMP. The pending state is also used when an operation is a reaction (threshold) operation waiting to be triggered. You can schedule a single IP SLAs operation or a group of operations at one time.

You can schedule several IP SLAs operations by using a single command through the Cisco IOS CLI or the CISCO RTTMON-MIB. Scheduling the operations to run at evenly distributed times allows you to control the amount of IP SLAs monitoring traffic. This distribution of IP SLAs operations helps minimize the CPU utilization and thus improves network scalability.

For more details about the IP SLAs multioperations scheduling functionality, see the “IP SLAs—Multiple Operation Scheduling” chapter of the *Cisco IOS IP SLAs Configuration Guide* at this URL:


**IP SLAs Operation Threshold Monitoring**

To support successful service level agreement monitoring, you must have mechanisms that notify you immediately of any possible violation. IP SLAs can send SNMP traps that are triggered by events such as these:

- Connection loss
- Timeout
- Round-trip time threshold
- Average jitter threshold
- One-way packet loss
- One-way jitter
- One-way mean opinion score (MOS)
One-way latency

An IP SLAs threshold violation can also trigger another IP SLAs operation for further analysis. For example, the frequency could be increased or an ICMP path echo or ICMP path jitter operation could be initiated for troubleshooting.

Determining the type of threshold and the level to set can be complex, and depends on the type of IP service being used in the network. For more details on using thresholds with Cisco IOS IP SLAs operations, see the “IP SLAs—Proactive Threshold Monitoring” chapter of the Cisco IOS IP SLAs Configuration Guide at this URL:


Configuring IP SLAs Operations

This section does not include configuration information for all available operations as the configuration information details are included in the Cisco IOS IP SLAs Configuration Guide. It does include several operations as examples, including configuring the responder, configuring UDP jitter operation, which requires a responder, and configuring ICMP echo operation, which does not require a responder. For details about configuring other operations, see the Cisco IOS IP SLAs Configuration Guide at this URL


This section includes this information:

- Default Configuration, page 41-6
- Configuration Guidelines, page 41-6
- Configuring the IP SLAs Responder, page 41-7
- Analyzing IP Service Levels by Using the UDP Jitter Operation, page 41-8
- Analyzing IP Service Levels by Using the ICMP Echo Operation, page 41-11

Default Configuration

No IP SLAs operations are configured.

Configuration Guidelines

For information on the IP SLAs commands, see the Cisco IOS IP SLAs Command Reference, Release 12.4T command reference at this URL:


For detailed descriptions and configuration procedures, see the Cisco IOS IP SLAs Configuration Guide, Release 12.4T at this URL:


Note that not all of the IP SLAs commands or operations described in this guide are supported on the switch. The switch supports IP service level analysis by using UDP jitter, UDP echo, HTTP, TCP connect, ICMP echo, ICMP path echo, ICMP path jitter, FTP, DNS, and DHCP, as well as multiple operation scheduling and proactive threshold monitoring. It does not support VoIP service levels using the gatekeeper registration delay operations measurements.
Before configuring any IP SLAs application, you can use the **show ip sla application** privileged EXEC command to verify that the operation type is supported on your software image. This is an example of the output from the command:

```
Switch# show ip sla application
  IP SLAs
Version: 2.2.0 Round Trip Time MIB, Infrastructure Engine-II
Time of last change in whole IP SLAs: 22:17:39.117 UTC Fri Jun
Estimated system max number of entries: 15801

Estimated number of configurable operations: 15801
Number of Entries configured : 0
Number of active Entries      : 0
Number of pending Entries     : 0
Number of inactive Entries    : 0

Supported Operation Types
Type of Operation to Perform: 802.1agEcho
Type of Operation to Perform: 802.1agJitter
Type of Operation to Perform: dhcp
Type of Operation to Perform: dns
Type of Operation to Perform: echo
Type of Operation to Perform: ftp
Type of Operation to Perform: http
Type of Operation to Perform: jitter
Type of Operation to Perform: pathEcho
Type of Operation to Perform: pathJitter
Type of Operation to Perform: tcpConnect
Type of Operation to Perform: udpEcho

IP SLAs low memory water mark: 21741224
```

### Configuring the IP SLAs Responder

The IP SLAs responder is available only on Cisco IOS software-based devices, including some Layer 2 switches that do not support full IP SLAs functionality, such as the Catalyst 2960 or the Cisco ME 2400 switch. Beginning in privileged EXEC mode, follow these steps to configure the IP SLAs responder on the target device (the operational target):

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>ip sla responder {tcp-connect</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The IP address and port number must match those configured on the source device for the IP SLAs operation.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>end</td>
</tr>
</tbody>
</table>
### Configuring IP SLAs Operations

To disable the IP SLAs responder, enter the `no ip sla responder` global configuration command. This example shows how to configure the device as a responder for the UDP jitter IP SLAs operation in the next procedure:

```
Switch(config)# ip sla responder udp-echo 172.29.139.134 5000
```

### Analyzing IP Service Levels by Using the UDP Jitter Operation

Jitter means interpacket delay variance. When multiple packets are sent consecutively 10 ms apart from source to destination, if the network is behaving correctly, the destination should receive them 10 ms apart. But if there are delays in the network (like queuing, arriving through alternate routes, and so on) the arrival delay between packets might be more than or less than 10 ms with a positive jitter value meaning that the packets arrived more than 10 ms apart. If the packets arrive 12 ms apart, positive jitter is 2 ms; if the packets arrive 8 ms apart, negative jitter is 2 ms. For delay-sensitive networks, positive jitter values are undesirable, and a jitter value of 0 is ideal.

In addition to monitoring jitter, the IP SLAs UDP jitter operation can be used as a multipurpose data gathering operation. The packets IP SLAs generates carry packet sending and receiving sequence information and sending and receiving time stamps from the source and the operational target. Based on these, UDP jitter operations measure this data:

- Per-direction jitter (source to destination and destination to source)
- Per-direction packet-loss
- Per-direction delay (one-way delay)
- Round-trip delay (average round-trip time)

Because the paths for the sending and receiving of data can be different (asymmetric), you can use the per-direction data to more readily identify where congestion or other problems are occurring in the network.

The UDP jitter operation generates synthetic (simulated) UDP traffic and sends a number of UDP packets, each of a specified size, sent a specified number of milliseconds apart, from a source router to a target router, at a given frequency. By default, ten packet-frames, each with a payload size of 10 bytes are generated every 10 ms, and the operation is repeated every 60 seconds. You can configure each of these parameters to best simulate the IP service you want to provide.

To provide accurate one-way delay (latency) measurements, time synchronization, such as that provided by NTP, is required between the source and the target device. Time synchronization is not required for the one-way jitter and packet loss measurements. If the time is not synchronized between the source and target devices, one-way jitter and packet loss data is returned, but values of 0 are returned for the one-way delay measurements provided by the UDP jitter operation.

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>show ip sla responder</code></td>
<td>Verify the IP SLAs responder configuration on the device.</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

**Note**

Before you configure a UDP jitter operation on the source device, you must enable the IP SLAs responder on the target device (the operational target).
Beginning in privileged EXEC mode, follow these steps to configure UDP jitter operation on the source device:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 ip sla operation-number</td>
<td>Create an IP SLAs operation, and enter IP SLAs configuration mode.</td>
</tr>
<tr>
<td>Step 3 udp-jitter {destination-ip-address</td>
<td>Configure the IP SLAs operation as a UDP jitter operation, and enter UDP jitter configuration mode.</td>
</tr>
<tr>
<td>destination-hostname} destination-port [source-ip [ip-address</td>
<td>[source-port port-number] [control {enable</td>
</tr>
<tr>
<td>destination-hostname]</td>
<td>destination-ip-address</td>
</tr>
<tr>
<td>destination-port—Specify</td>
<td>destination-hostname—Specify the destination IP address or hostname. When a source IP address or hostname is not specified, IP SLAs chooses the IP address nearest to the destination.</td>
</tr>
<tr>
<td>the destination port</td>
<td>destination-port—Specify the destination port number in the range from 1 to 65535.</td>
</tr>
<tr>
<td>number in the range from</td>
<td>(Optional) source-ip [ip-address</td>
</tr>
<tr>
<td>1 to 65535.</td>
<td>destination-hostname]—Specify the source IP address or hostname. When a source IP address or hostname is not specified, IP SLAs chooses the IP address nearest to the destination.</td>
</tr>
<tr>
<td>(Optional) source-port</td>
<td>(Optional) control—Enable or disable sending of IP SLAs control messages to the IP SLAs responder. By default, IP SLAs control messages are sent to the destination device to establish a connection with the IP SLAs responder.</td>
</tr>
<tr>
<td>port-number—Specify the</td>
<td>(Optional) num-packets number-of-packets—Enter the number of packets to be generated. The range is 1 to 6000; the default is 10.</td>
</tr>
<tr>
<td>source port number in the</td>
<td>(Optional) interval interpacket-interval—Enter the interval between sending packets in milliseconds. The range is 1 to 6000; the default value is 20 ms.</td>
</tr>
<tr>
<td>range from 1 to 65535.</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>Step 4 frequency seconds</td>
<td>(Optional) Set the rate at which a specified IP SLAs operation repeats. The range is from 1 to 604800 seconds; the default is 60 seconds.</td>
</tr>
<tr>
<td>Step 5 exit</td>
<td>Exit UDP jitter configuration mode, and return to global configuration mode.</td>
</tr>
</tbody>
</table>
### Chapter 41      Configuring Cisco IOS IP SLAs Operations

#### Configuring IP SLAs Operations

**To disable the IP SLAs operation,** enter the `no ip sla operation-number` global configuration command.

This example shows how to configure a UDP jitter IP SLAs operation:

```
Switch(config)# ip sla 10
Switch(config-ip-sla)# udp-jitter 172.29.139.134 5000
Switch(config-ip-sla-jitter)# frequency 30
Switch(config-ip-sla-jitter)# exit
Switch(config)# ip sla schedule 5 start-time now life forever
Switch(config)# end
Switch# show ip sla configuration 10
```

**Step 6**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`ip sla monitor schedule operation-number life [forever</td>
<td>seconds]] [start-time [hh:mm [:ss] [month day</td>
</tr>
</tbody>
</table>

- **operation-number** — Enter the RTR entry number.
- **life** — Set the operation to run indefinitely (*forever*) or for a specific number of *seconds*. The range is from 0 to 2147483647. The default is 3600 seconds (1 hour).
- **start-time** — Enter *pending* to select no information collection until a start time is selected.
- **ageout seconds** — Enter the number of seconds to keep the operation in memory when it is not actively collecting information. The range is 0 to 2073600 seconds, the default is 0 seconds (never ages out).
- **recurring** — Set the operation to automatically run every day.

**Step 7**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

**Step 8**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip sla configuration [operation-number]</code></td>
<td>(Optional) Display configuration values, including all defaults for all IP SLAs operations or a specified operation.</td>
</tr>
</tbody>
</table>

**Step 9**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable the IP SLAs operation, enter the `no ip sla operation-number` global configuration command. This example shows how to configure a UDP jitter IP SLAs operation:

```
Switch(config)# ip sla 10
Switch(config-ip-sla)# udp-jitter 172.29.139.134 5000
Switch(config-ip-sla-jitter)# frequency 30
Switch(config-ip-sla-jitter)# exit
Switch(config)# ip sla schedule 5 start-time now life forever
Switch(config)# end
Switch# show ip sla configuration 10
IP SLAs, Infrastructure Engine-II.
```

Entry number: 10
### Configuring IP SLAs Operations

Owner:
Tag:
Type of operation to perform: udp-jitter
Target address/Source address: 1.1.1.1/0.0.0.0
Target port/Source port: 2/0
Request size (ARR data portion): 32
Operation timeout (milliseconds): 5000
Packet Interval (milliseconds)/Number of packets: 20/10
Type Of Service parameters: 0x0
Verify data: No
Vrf Name:
Control Packets: enabled
Schedule:
  Operation frequency (seconds): 30
  Next Scheduled Start Time: Pending trigger
  Group Scheduled : FALSE
  Randomly Scheduled : FALSE
  Life (seconds): 3600
  Entry Ageout (seconds): never
  Recurring (Starting Everyday): FALSE
  Status of entry (SNMP RowStatus): notInService
Threshold (milliseconds): 5000
Distribution Statistics:
  Number of statistic hours kept: 2
  Number of statistic distribution buckets kept: 1
  Statistic distribution interval (milliseconds): 20
Enhanced History:

### Analyzing IP Service Levels by Using the ICMP Echo Operation

The ICMP echo operation measures end-to-end response time between a Cisco device and any devices using IP. Response time is computed by measuring the time taken between sending an ICMP echo request message to the destination and receiving an ICMP echo reply. Many customers use IP SLAs ICMP-based operations, in-house ping testing, or ping-based dedicated probes for response time measurements between the source IP SLAs device and the destination IP device. The IP SLAs ICMP echo operation conforms to the same specifications as ICMP ping testing, and the two methods result in the same response times.

**Note**
This operation does not require the IP SLAs responder to be enabled.

Beginning in privileged EXEC mode, follow these steps to configure an ICMP echo operation on the source device:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip sla operation-number</td>
<td>Create an IP SLAs operation and enter IP SLAs configuration mode.</td>
</tr>
</tbody>
</table>
Chapter 41 Configuring Cisco IOS IP SLAs Operations

Configuring IP SLAs Operations

To disable the IP SLAs operation, enter the no ip sla operation-number global configuration command. This example shows how to configure an ICMP echo IP SLAs operation:

```
Switch(config)# ip sla 12
Switch(config-ip-sla)# icmp-echo 172.29.139.134
Switch(config-ip-sla-echo)# frequency 30
Switch(config-ip-sla-echo)# exit
Switch(config)# ip sla schedule 5 start-time now life forever
```

### Command Purpose

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3</td>
<td><strong>icmp-echo</strong> *(destination-ip-address</td>
</tr>
<tr>
<td></td>
<td>Configure the IP SLAs operation as an ICMP Echo operation and enter ICMP echo configuration mode.</td>
</tr>
<tr>
<td></td>
<td>• destination-ip-address</td>
</tr>
<tr>
<td></td>
<td>• (Optional) source-ip (ip-address</td>
</tr>
<tr>
<td></td>
<td>• (Optional) source-interface interface-id—Specify the source interface for the operation.</td>
</tr>
<tr>
<td>Step 4</td>
<td><strong>frequency seconds</strong></td>
</tr>
<tr>
<td></td>
<td>(Optional) Set the rate at which a specified IP SLAs operation repeats. The range is from 1 to 604800 seconds; the default is 60 seconds.</td>
</tr>
<tr>
<td>Step 5</td>
<td><strong>exit</strong></td>
</tr>
<tr>
<td></td>
<td>Exit UDP jitter configuration mode, and return to global configuration mode.</td>
</tr>
<tr>
<td>Step 6</td>
<td><strong>ip sla schedule</strong> operation-number [life [forever</td>
</tr>
<tr>
<td></td>
<td>Configure the scheduling parameters for an individual IP SLAs operation.</td>
</tr>
<tr>
<td></td>
<td>• operation-number—Enter the RTR entry number.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) life—Set the operation to run indefinitely (forever) or for a specific number of seconds. The range is from 0 to 2147483647. The default is 3600 seconds (1 hour)</td>
</tr>
<tr>
<td></td>
<td>• (Optional) start-time—Enter the time for the operation to begin collecting information:</td>
</tr>
<tr>
<td></td>
<td>• To start at a specific time, enter the hour, minute, second (in 24-hour notation), and day of the month. If no month is entered, the default is the current month.</td>
</tr>
<tr>
<td></td>
<td>• Enter pending to select no information collection until a start time is selected.</td>
</tr>
<tr>
<td></td>
<td>• Enter now to start the operation immediately.</td>
</tr>
<tr>
<td></td>
<td>• Enter after hh:mm:ss to indicate that the operation should start after the entered time has elapsed.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) ageout seconds—Enter the number of seconds to keep the operation in memory when it is not actively collecting information. The range is 0 to 2073600 seconds; the default is 0 seconds (never ages out).</td>
</tr>
<tr>
<td></td>
<td>• (Optional) recurring—Set the operation to automatically run every day.</td>
</tr>
<tr>
<td>Step 7</td>
<td><strong>end</strong></td>
</tr>
<tr>
<td></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 8</td>
<td><strong>show ip sla configuration</strong> [operation-number]</td>
</tr>
<tr>
<td></td>
<td>(Optional) Display configuration values including all defaults for all IP SLAs operations or a specified operation.</td>
</tr>
<tr>
<td>Step 9</td>
<td><strong>copy running-config startup-config</strong></td>
</tr>
<tr>
<td></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
Monitoring IP SLAs Operations

Use the User EXEC or Privileged EXEC commands in Table 41-1 to display IP SLAs operations configuration and results.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip sla application</td>
<td>Display global information about Cisco IOS IP SLAs.</td>
</tr>
<tr>
<td>show ip sla authentication</td>
<td>Display IP SLAs authentication information.</td>
</tr>
<tr>
<td>show ip sla configuration [entry-number]</td>
<td>Display configuration values including all defaults for all IP SLAs operations or a specific operation.</td>
</tr>
<tr>
<td>show ip sla enhanced-history {collection-statistics</td>
<td>distribution statistics} [entry-number]</td>
</tr>
<tr>
<td>show ip sla ethernet-monitor configuration [entry-number]</td>
<td>Display IP SLAs automatic Ethernet configuration.</td>
</tr>
<tr>
<td>show ip sla group schedule [schedule-entry-number]</td>
<td>Display IP SLAs group scheduling configuration and details.</td>
</tr>
<tr>
<td>show ip sla history [entry-number</td>
<td>full</td>
</tr>
</tbody>
</table>
**Table 41-1 Monitoring IP SLAs Operations (continued)**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip sla mpls-lsp-monitor { collection-statistics</td>
<td>configuration</td>
</tr>
<tr>
<td>show ip sla reaction-configuration [entry-number]</td>
<td>Display the configured proactive threshold monitoring settings for all IP SLAs operations or a specific operation.</td>
</tr>
<tr>
<td>show ip sla reaction-trigger [entry-number]</td>
<td>Display the reaction trigger information for all IP SLAs operations or a specific operation.</td>
</tr>
<tr>
<td>show ip sla responder</td>
<td>Display information about the IP SLAs responder.</td>
</tr>
<tr>
<td>show ip sla statistics [entry-number</td>
<td>aggregated</td>
</tr>
</tbody>
</table>

**Understanding TWAMP**

TWAMP consists of two related protocols. Use the TWAMP-Control protocol to start performance measurement sessions. Use TWAMP-Test to send and receive performance-measurement probes. You can deploy TWAMP in a simplified network architecture, with the control-client and the session-sender on one device and the server and the session-reflector on another device.

The Cisco IOS software TWAMP implementation supports a basic configuration. Figure 41-3 shows a sample deployment.

Figure 41-4 shows the four logical entities that comprise TWAMP.

**Figure 41-3 TWAMP Deployment**

![TWAMP Deployment Diagram]
Figure 41-4 TWAMP Architecture

![TWAMP Architecture Diagram]

Although each entity is separate, the protocol allows for logical merging of the roles on a single device.

### Configuring TWAMP

- Configuring the TWAMP Server, page 41-15
- Configuring the TWAMP Reflector, page 41-16
- Troubleshooting TWAMP, page 41-16

### Configuring the TWAMP Server

The TWAMP server and reflector functionality are configured on the same device.

> **Note**
> The switch does not support the TWAMP sender and client roles.

Beginning in privileged EXEC mode, follow these steps to configure the TWAMP server:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong> Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>ip sla server twamp</strong> Configure the switch as a TWAMP server, and enter TWAMP configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>port port-number</strong> (Optional) Specify the port to be used by the TWAMP server to listen for connection and control requests. The same port negotiates for the port to which performance probes are sent. The configured port should not be an IANA well-known port or any port used by other applications. The default is port 862.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>timer inactivity seconds</strong> (Optional) Set the maximum time, in seconds, the session can be inactive before the session ends. The range is 1–6000 seconds. The default is 900 seconds.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>end</strong> Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 6s</strong></td>
<td><strong>show ip sla standards</strong> (Optional) Display the IP SLA standards supported on the switch.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>show ip sla twamp connection requests</strong> (Optional) Display the number and the source of TWAMP connections.</td>
</tr>
</tbody>
</table>
To disable the IP SLA TWAMP server, enter the `no ip sla server twamp` global configuration command. This example shows how to configure a switch as an IP SLA TWAMP server:

```
Switch(config)# ip sla server twamp
Switch(config-twamp-srvr)# port 9000
Switch(config-twamp-srvr)# timer inactivity 300
```

### Configuring the TWAMP Reflector

The TWAMP server and reflector functionality are both configured on the same device. Beginning in privileged EXEC mode, follow these steps to configure the TWAMP reflector:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 ip sla responder twamp</td>
<td>Configure the switch as a TWAMP responder, and enter TWAMP configuration mode.</td>
</tr>
<tr>
<td>Step 3 timeout <code>seconds</code></td>
<td>(Optional) Set the maximum time, in seconds, the session can be inactive before the session ends. The range is 1–604800 seconds. The default is 900 seconds.</td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5 show ip sla twamp session [source-ip <code>ip-address</code> source-port <code>port-number</code>]</td>
<td>(Optional) Display information about TWAMP test results for the specified client.</td>
</tr>
<tr>
<td>Step 6 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable the IP SLA TWAMP reflector, enter the `no ip sla responder twamp` global configuration command. This example shows how to configure a switch as an IP SLA TWAMP reflector:

```
Switch(config)# ip sla responder twamp
Switch(config-twamp-srvr)# timeout 300
```

### Troubleshooting TWAMP

Use these commands to troubleshoot TWAMP sessions:

- `debug ip sla error twamp [connection source-ip `ip-address` | control {reflector | server} | session source-ip `ip-address`]
- `debug ip sla trace twamp [connection source-ip `ip-address` | control {reflector | server} | session source-ip `ip-address`]`
Configuring Enhanced Object Tracking

This chapter describes how to configure enhanced object tracking on the Catalyst 3750 Metro switch. This feature provides a more complete alternative to the Hot Standby Routing Protocol (HSRP) tracking mechanism, which allows you to track the line-protocol state of an interface. If the line protocol state of an interface goes down, the HSRP priority of the interface is reduced and another HSRP device with a higher priority becomes active. The enhanced object tracking feature separates the tracking mechanism from HSRP and creates a separate, standalone tracking process that can be used by processes other than HSRP. This allows tracking other objects in addition to the interface line-protocol state. A client process, such as HSRP or Gateway Local Balancing Protocol (GLBP), can register an interest in tracking objects and request notification when the tracked object changes state. This feature increases the availability and speed of recovery of a routing system and decreases outages and outage duration.

For more information about enhanced object tracking and the commands used to configure it, see this URL:


The chapter includes these sections:

- Understanding Enhanced Object Tracking, page 42-1
- Configuring Enhanced Object Tracking Features, page 42-2
- Monitoring Enhanced Object Tracking, page 42-13

Understanding Enhanced Object Tracking

Each tracked object has a unique number that is specified in the tracking command-line interface (CLI). Client processes use this number to track a specific object. The tracking process periodically polls the tracked object for value changes and sends any changes (as up or down values) to interested client processes, either immediately or after a specified delay. Several clients can track the same object, and can take different actions when the object changes state.

You can also track a combination of objects in a list by using either a weight threshold or a percentage threshold to measure the state of the list. You can combine objects using Boolean logic. A tracked list with a Boolean “AND” function requires that each object in the list be in an up state for the tracked object to be up. A tracked list with a Boolean “OR” function needs only one object in the list to be in the up state for the tracked object to be up.
Configuring Enhanced Object Tracking Features

These sections describe configuring enhanced object tracking:

- Default Configuration, page 42-2
- Tracking Interface Line-Protocol or IP Routing State, page 42-2
- Configuring a Tracked List, page 42-3
- Configuring HSRP Object Tracking, page 42-7
- Configuring Other Tracking Characteristics, page 42-8
- Configuring IP SLAs Object Tracking, page 42-8
- Configuring Static Routing Support, page 42-10

Default Configuration

No type of object tracking is configured.

Tracking Interface Line-Protocol or IP Routing State

You can track either the interface line protocol state or the interface IP routing state. When you track the IP routing state, these three conditions are required for the object to be up:

- IP routing must be enabled and active on the interface.
- The interface line-protocol state must be up.
- The interface IP address must be known.

If all three of these conditions are not met, the IP routing state is down.

Beginning in privileged EXEC mode, follow these steps to track the line-protocol state or IP routing state of an interface:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>track object-number interface-id line-protocol</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>delay {up seconds [down seconds]}</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>exit</td>
</tr>
<tr>
<td>Step 5</td>
<td>track object-number interface-id ip routing</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
This example configures the tracking of an interface line-protocol state and verifies the configuration:

```
Switch(config)# track 33 interface gigabitethernet 1/0/1 line-protocol
Switch(config-track)# end
Switch# show track 33
Track 33
  Interface GigabitEthernet1/0/1 line-protocol
  Line protocol is Down (hw down)
  1 change, last change 00:18:28
```

### Configuring a Tracked List

You can configure a tracked list of objects with a Boolean expression, a weight threshold, or a percentage threshold. A tracked list contains one or more objects. An object must exist before it can be added to the tracked list.

- You configure a Boolean expression to specify calculation by using either “AND” or “OR” operators.
- When you measure the tracked list state by a weight threshold, you assign a weight number to each object in the tracked list. The state of the tracked list is determined by whether or not the threshold was met. The state of each object is determined by comparing the total weight of all objects against a threshold weight for each object.
- When you measure the tracked list by a percentage threshold, you assign a percentage threshold to all objects in the tracked list. The state of each object is determined by comparing the assigned percentages of each object to the list.

### Configuring a Tracked List with a Boolean Expression

Configuring a tracked list with a Boolean expression enables calculation by using either “AND” or “OR” operators. For example, when tracking two interfaces using the “AND” operator, \(up\) means that both interfaces are up, and \(down\) means that either interface is down.
Beginning in privileged EXEC mode, follow these steps to configure a tracked list of objects with a Boolean expression:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> track track-number list boolean [and</td>
<td>or]</td>
</tr>
<tr>
<td></td>
<td>- <strong>boolean</strong>—Specify the state of the tracked list based on a Boolean calculation.</td>
</tr>
<tr>
<td></td>
<td>- <strong>and</strong>—Specify that the list is up if all objects are up or down if one or more objects are down.</td>
</tr>
<tr>
<td></td>
<td>- <strong>or</strong>—Specify that the list is up if one object is up or down if all objects are down.</td>
</tr>
<tr>
<td><strong>Step 3</strong> object object-number [not]</td>
<td>Specify the object to be tracked. The range is from 1 to 500. The keyword <strong>not</strong> negates the state of the object, which means that when the object is up, the tracked list detects the object as down.</td>
</tr>
<tr>
<td><strong>Step 4</strong> delay {up seconds [down seconds]</td>
<td>[up seconds] down seconds}</td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 6</strong> show track object-number</td>
<td>Verify that the specified objects are being tracked.</td>
</tr>
<tr>
<td><strong>Step 7</strong> copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Use the **no track track-number** global configuration command to delete the tracked list.

This example configures track list 4 with a Boolean AND expression that contains two objects with one object state negated. If the list is up, the list detects that object 2 is down:

```
Switch(config)# track 4 list boolean and
Switch(config-track)# object 1
Switch(config-track)# object 2 not
Switch(config-track)# exit
```

### Configuring a Tracked List with a Weight Threshold

To track by weight threshold, configure a tracked list of objects, specify that weight is used as the threshold, and configure a weight for each of its objects. The state of each object is determined by comparing the total weight of all objects that are up against a threshold weight for each object.

You cannot use the Boolean “NOT” operator in a weight threshold list.
Beginning in privileged EXEC mode, follow these steps to configure a tracked list of objects by using a weight threshold and to configure a weight for each object:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>track track-number list threshold weight</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>object object-number [weight weight-number]</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>threshold weight {up number</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>delay {up seconds [down seconds]</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>show track object-number</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

Use the no track track-number global configuration command to delete the tracked list.

The example configures track list 4 to track by weight threshold. If object 1 and object 2 are down, then track list 4 is up because object 3 satisfies the up threshold value of up 30. But if object 3 is down, both objects 1 and 2 must be up in order to satisfy the threshold weight.

```
Switch(config)# track 4 list threshold weight
Switch(config-track)# object 1 weight 15
Switch(config-track)# object 2 weight 20
Switch(config-track)# object 3 weight 30
Switch(config-track)# threshold weight up 30 down 10
Switch(config-track)# exit
```

This configuration can be useful if object 1 and object 2 represent two small bandwidth connections and object 3 represents one large bandwidth connection. The configured down 10 value means that once the tracked object is up, it will not go down until the threshold value is equal to or lower than 10, which in this example means that all connections are down.
Configuring a Tracked List with a Percentage Threshold

To track by percentage threshold, configure a tracked list of objects, specify that a percentage will be used as the threshold, and specify a percentage for all objects in the list. The state of the list is determined by comparing the assigned percentage of each object to the list.

You cannot use the Boolean “NOT” operator in a percentage threshold list.

Beginning in privileged EXEC mode, follow these steps to configure a tracked list of objects by using a percentage threshold:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>track track-number list threshold percentage</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>object object-number</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>threshold percentage {up number}</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>delay {up seconds} [down seconds]</td>
</tr>
<tr>
<td>Step 6</td>
<td>end</td>
</tr>
<tr>
<td>Step 7</td>
<td>show track object-number</td>
</tr>
<tr>
<td>Step 8</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

Use the no track track-number global configuration command to delete the tracked list.

This example configures tracked list 4 with three objects and a specified percentages to measure the state of the list:

```
Switch(config)# track 4 list threshold percentage
Switch(config-track)# object 1
Switch(config-track)# object 2
Switch(config-track)# object 3
Switch(config-track)# threshold percentage up 51 down 10
Switch(config-track)# exit
```
Configuring HSRP Object Tracking

Beginning in privileged EXEC mode, follow these steps to configure a standby HSRP group to track an object and change the HSRP priority based on the object state:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>track object-number {interface interface-id {line-protocol</td>
</tr>
<tr>
<td></td>
<td>• The object-number range is from 1 to 500.</td>
</tr>
<tr>
<td></td>
<td>• Enter interface interface-id to select an interface to track.</td>
</tr>
<tr>
<td></td>
<td>• Enter line-protocol to track the interface line protocol state or enter ip routing to track the interface IP routing state.</td>
</tr>
<tr>
<td></td>
<td>• Enter ip route ip-address/prefix-length to track the state of an IP route.</td>
</tr>
<tr>
<td></td>
<td>• Enter metric threshold to track the threshold metric or enter reachability to track if the route is reachable.</td>
</tr>
<tr>
<td></td>
<td>• Enter list to track objects grouped in a list. Configure the list as described on the previous pages.</td>
</tr>
<tr>
<td></td>
<td>• For boolean, see the “Configuring a Tracked List with a Boolean Expression” section on page 42-3</td>
</tr>
<tr>
<td></td>
<td>• For threshold weight, see the “Configuring a Tracked List with a Weight Threshold” section on page 42-4</td>
</tr>
<tr>
<td></td>
<td>• For threshold percentage, see the “Configuring a Tracked List with a Percentage Threshold” section on page 42-6</td>
</tr>
<tr>
<td>Note</td>
<td>Repeat this step for each interface to be tracked.</td>
</tr>
<tr>
<td>Step 3</td>
<td>exit Return to global configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>interface interface-id Enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 5</td>
<td>standby [group-number] ip [ip-address [secondary]] Create (or enable) the HSRP group by using its number and virtual IP address.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) group-number—Enter a group number on the interface for which HSRP is being enabled. The range is 0 to 255; the default is 0. If there is only one HSRP group, you do not need to enter a group number.</td>
</tr>
<tr>
<td></td>
<td>• (Optional on all but one interface) ip-address—Specify the virtual IP address of the hot standby router interface. You must enter the virtual IP address for at least one of the interfaces; it can be learned on the other interfaces.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) secondary—Specify that the IP address is a secondary hot standby router interface. If this keyword is omitted, the configured address is the primary IP address.</td>
</tr>
</tbody>
</table>
Chapter 42  Configuring Enhanced Object Tracking

### Configuring Enhanced Object Tracking Features

You can also use the enhanced object tracking for tracking other characteristics.

- You can track the reachability of an IP route by using the `track ip route reachability` global configuration command.
- You can use the `track ip route metric threshold` global configuration command to determine if a route is above or below threshold.
- You can use the `track resolution` global configuration command to change the metric resolution default values for routing protocols.
- You can use the `track timer` tracking configuration command to configure the tracking process to periodically poll tracked objects.

Use the `show track` privileged EXEC command to verify enhanced object tracking configuration.

For more information about enhanced object tracking and the commands used to configure it, see this URL:


### Configuring Other Tracking Characteristics

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
|        | `standby [group-number] track object-number [decrement [priority-decrement]]` | Configure HSRP to track an object and change the hot standby priority based on the state of the object.  
- (Optional) `group-number`—Enter the group number to which the tracking applies.  
- `object-number`—Enter a number representing the object to be tracked. The range is from 1 to 500; the default is 1.  
- (Optional) `decrement priority-decrement`—Specify the amount by which the hot standby priority for the router is decremented (or incremented) when the tracked object goes down (or comes back up). The range is from 1 to 255; the default is 10. |

| Step 7 | `end`                                         | Return to privileged EXEC mode.                                          |
| Step 8 | `show standby`                                | Verify the standby router IP address and tracking states.               |
| Step 9 | `copy running-config startup-config`         | (Optional) Save your entries in the configuration file.                 |

### Configuring IP SLAs Object Tracking

Cisco IOS IP Service Level Agreements (IP SLAs) is a network performance measurement and diagnostics tool that uses active monitoring by generating traffic to measure network performance. Cisco IP SLAs operations collects real-time metrics that you can use for network troubleshooting, design, and analysis.

For more information about Cisco IP SLAs on the switch, see Chapter 41, “Configuring Cisco IOS IP SLAs Operations.” For IP SLAs command information see the `Cisco IOS IP SLAs Command Reference` at this URL:


Object tracking of IP SLAs operations allows clients to track the output from IP SLAs objects and use this information to trigger an action. Every IP SLAs operation maintains an SNMP operation return-code value, such as `OK` or `OverThreshold`, that can be interpreted by the tracking process. You can track two
aspects of IP SLAs operation: state and reachability. For state, if the return code is OK, the track state is up; if the return code is not OK, the track state is down. For reachability, if the return code is OK or OverThreshold, reachability is up; if not OK, reachability is down.

Beginning in privileged EXEC mode, follow these steps to track the state of an IP SLAs operation or the reachability of an IP SLAs IP host:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>track object-number rtr operation-number state</td>
</tr>
<tr>
<td></td>
<td><strong>(Optional)</strong> Specify a period of time in seconds to delay communicating state changes of a tracked object. The range is from 1 to 180 seconds.</td>
</tr>
<tr>
<td>Step 3</td>
<td>delay {up seconds [down seconds]</td>
</tr>
<tr>
<td></td>
<td>[up seconds] down seconds}</td>
</tr>
<tr>
<td>Step 4</td>
<td>exit</td>
</tr>
<tr>
<td>Step 5</td>
<td>track object-number rtr operation-number reachability</td>
</tr>
<tr>
<td></td>
<td><strong>(Optional)</strong> Specify a period of time in seconds to delay communicating state changes of a tracked object. The range is from 1 to 180 seconds.</td>
</tr>
<tr>
<td>Step 6</td>
<td>delay {up seconds [down seconds]</td>
</tr>
<tr>
<td></td>
<td>[up seconds] down seconds}</td>
</tr>
<tr>
<td>Step 7</td>
<td>end</td>
</tr>
<tr>
<td>Step 8</td>
<td>show track object-number</td>
</tr>
<tr>
<td>Step 9</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

This example shows how to configure and display IP SLAs state tracking:

```
Switch(config)# track 2 200 state
Switch(config)# end
Switch# show track 2
Track 2
 Response Time Reporter 1 state
 State is Down
  1 change, last change 00:00:47
 Latest operation return code: over threshold
 Latest RTT (millisecs) 4
 Tracked by:
      HSRP Ethernet0/1 3
```

This example output shows whether a route is reachable:

```
Switch(config)# track 3 500 reachability
Switch(config)# end
Switch# show track 3
Track 3
 Response Time Reporter 1 reachability
 Reachability is Up
  1 change, last change 00:00:47
 Latest operation return code: over threshold
 Latest RTT (millisecs) 4
 Tracked by:
      HSRP Ethernet0/1 3
```
**Configuring Static Routing Support**

Switches that are running Cisco IOS release 12.2(46)SE or later support enhanced object tracking static routing. Static routing support using enhanced object tracking provides the ability for the switch to use ICMP pings to identify when a preconfigured static route or a DHCP route goes down. When tracking is enabled, the system tracks the state of the route and informs the client when that state changes. Static route object tracking uses Cisco IP SLAs to generate ICMP pings to monitor the state of the connection to the primary gateway.

- For more information about Cisco IP SLAs support on the switch, see Chapter 41, “Configuring Cisco IOS IP SLAs Operations.”
- For more information about static route object tracking, see this URL:
  

You use this process to configure static route object tracking:

**Step 1** Configure a primary interface for static routing or for DHCP.

**Step 2** Configure an IP SLAs agent to ping an IP address using a primary interface and a track object to monitor the state of the agent.

**Step 3** Configure a default static default route using a secondary interface. This route is used only if the primary route is removed.

### Configuring a Primary Interface

Beginning in privileged EXEC mode, follow these steps to configure a primary interface for static routing:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> interface interface-id</td>
<td>Select a primary or secondary interface and enter interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong> description string</td>
<td>Add a description to the interface.</td>
</tr>
<tr>
<td><strong>Step 4</strong> ip address ip-address mask [secondary]</td>
<td>Set the primary or secondary IP address for the interface.</td>
</tr>
<tr>
<td><strong>Step 5</strong> exit</td>
<td>Return to global configuration mode.</td>
</tr>
</tbody>
</table>

Beginning in privileged EXEC mode, follow these steps to configure a primary interface for DHCP:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> interface interface-id</td>
<td>Select a primary or secondary interface and enter interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong> description string</td>
<td>Add a description to the interface.</td>
</tr>
<tr>
<td><strong>Step 4</strong> ip dhcp client route track number</td>
<td>Configure the DCHP client to associate any added routes with the specified track number. Valid numbers are from 1 to 500.</td>
</tr>
</tbody>
</table>
Beginning in privileged EXEC mode, follow these steps to configure network monitoring with Cisco IP SLAs:

### Command Purpose

**Step 1**
configure terminal

Enter global configuration mode.

**Step 2**
`ip sla operation-number`

Begin configuring a Cisco IP SLAs operation and enter IP SLA configuration mode.

**Step 3**
`icmp-echo`

Configure a Cisco IP SLAs end-to-end ICMP echo response time operation and enter IP SLAs ICMP echo configuration mode.

**Step 4**
`timeout milliseconds`

Set the amount of time for which the operation waits for a response from its request packet.

**Step 5**
`frequency seconds`

Set the rate at which the operation is sent into the network.

**Step 6**
`threshold milliseconds`

Set the rising threshold (hysteresis) that generates a reaction event and stores history information for the operation.

**Step 7**
`exit`

Exit IP SLAs ICMP echo configuration mode.

**Step 8**
`ip sla schedule operation-number [life [forever | seconds]] start-time time | pending | now | after time] [ageout seconds] [recurring]`

Configure the scheduling parameters for a single IP SLAs operation.

**Step 9**
`track object-number rtr operation-number | state | reachability`

Track the state of a Cisco IOS IP SLAs operation and enter tracking configuration mode.

**Step 10**
`end`

Return to privileged EXEC mode.

**Step 11**
`show track object-number`

Display tracking information to verify the configuration.

**Step 12**
`copy running-config startup-config`

(Optional) Save your entries in the configuration file.
### Configuring Enhanced Object Tracking Features

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>route-map map-tag [permit</td>
<td>deny] [sequence-number]</td>
</tr>
<tr>
<td>4</td>
<td>match ip address {access-list number</td>
<td>access-list name}</td>
</tr>
<tr>
<td>5</td>
<td>set ip next-hop dynamic dhcp</td>
<td>For DHCP networks only. Set the next hop to the gateway that was most recently learned by the DHCP client.</td>
</tr>
<tr>
<td>6</td>
<td>set interface interface-id</td>
<td>For static routing networks only. Indicate where to send output packets that pass a match clause of a route map for policy routing.</td>
</tr>
<tr>
<td>7</td>
<td>exit</td>
<td>Exit route-map configuration mode.</td>
</tr>
<tr>
<td>8</td>
<td>ip local policy route-map map-tag</td>
<td>Identify a route-map configuration mode.</td>
</tr>
<tr>
<td>9</td>
<td>ip route prefix mask {ip-address</td>
<td>interface-id [ip-address]} [distance] [name] [permanent</td>
</tr>
<tr>
<td>10</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>11</td>
<td>show ip route track table</td>
<td>Display information about the IP route track table.</td>
</tr>
<tr>
<td>12</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

For configuration examples, see this URL:

Monitoring Enhanced Object Tracking

Use the privileged EXEC or User EXEC commands in Table 42-1 to display enhanced object tracking information.

**Table 42-1  Commands for Displaying Tracking Information**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip route track table</code></td>
<td>Display information about the IP route track table.</td>
</tr>
<tr>
<td><code>show track [object-number]</code></td>
<td>Display information about the all tracking lists or the specified list.</td>
</tr>
<tr>
<td><code>show track brief</code></td>
<td>Display a single line of tracking information output.</td>
</tr>
<tr>
<td><code>show track interface [brief]</code></td>
<td>Display information about tracked interface objects.</td>
</tr>
<tr>
<td><code>show track ip [object-number] [brief] route</code></td>
<td>Display information about tracked IP-route objects.</td>
</tr>
<tr>
<td><code>show track resolution</code></td>
<td>Display the resolution of tracked parameters.</td>
</tr>
<tr>
<td><code>show track timers</code></td>
<td>Display tracked polling interval timers.</td>
</tr>
</tbody>
</table>
Configuring Ethernet OAM, CFM, and E-LMI

Ethernet Operations, Administration, and Maintenance (OAM) is a protocol for installing, monitoring, and troubleshooting Ethernet networks to increase management capability within the context of the overall Ethernet infrastructure. The Catalyst 3750 Metro switch supports IEEE 802.1ag Connectivity Fault Management (CFM), Ethernet Local Management Interface (E-LMI), and IEEE 802.3ah Ethernet OAM discovery, link monitoring, remote fault detection, and remote loopback. It also supports IP Service Level Agreements (SLAs) for CFM, and ITU-T Y.1731 fault management. Ethernet OAM manager controls the interworking between any two of the protocols (CFM, E-LMI, and OAM).

This chapter provides information about configuring CFM, E-LMI, and the Ethernet OAM protocol. It defines the differences between the ratified CFM 802.1ag standard (draft 8.1) and the previous version supported on the switch in Cisco IOS (draft 1.0). It also includes configuration information for CFM ITU-T Y.1731 fault management support in this release.

For complete command and configuration information for Ethernet OAM, CFM, E-LMI, and Y.1731, see the Cisco IOS Carrier Ethernet Configuration Guide at this URL:

For complete syntax of the commands used in this chapter, see the command reference for this release and the Cisco IOS Carrier Ethernet Command Reference at this URL:

Note
The Service Diagnostics 2.0 CFM diagnostic script is part of the 12.2(52)SE release. The script is available for download at:

Refer to the Service Diagnostic 2.0 user guide at:

This chapter contains these sections:

- Understanding Ethernet CFM, page 43-2
- Configuring Ethernet CFM, page 43-7
- Understanding CFM ITU-T Y.1731 Fault Management, page 43-23
- Configuring Y.1731 Fault Management, page 43-25
- Managing and Displaying Ethernet CFM Information, page 43-30
- Understanding the Ethernet OAM Protocol, page 43-32
- Setting Up and Configuring Ethernet OAM, page 43-33
- Displaying Ethernet OAM Protocol Information, page 43-42
- Understanding E-LMI, page 43-42
Understanding Ethernet CFM

Ethernet CFM is an end-to-end per-service-instance (per VLAN) Ethernet layer OAM protocol that includes proactive connectivity monitoring, fault verification, and fault isolation. End-to-end can be provider-edge-to-provider-edge (PE-to-PE) device or customer-edge-to customer-edge (CE-to-CE) device. Ethernet CFM, as specified by IEEE 802.1ag, is the standard for Layer 2 ping, Layer 2 traceroute, and end-to-end connectivity check of the Ethernet network.

These sections contain conceptual information about Ethernet CFM:

- CFM Domain, page 43-2
- Maintenance Associations and Maintenance Points, page 43-3
- CFM Messages, page 43-5
- Crosscheck Function and Static Remote MEPs, page 43-5
- SNMP Traps and Fault Alarms, page 43-5
- Configuration Error List, page 43-6
- CFM Version Interoperability, page 43-6
- IP SLAs Support for CFM, page 43-6

CFM Domain

A CFM maintenance domain is a management space on a network that is owned and operated by a single entity and defined by a set of ports internal to it, but at its boundary. You assign a unique maintenance level (from 0 to 7) to define the hierarchical relationship between domains. The larger the domain, the higher the level. For example, as shown in Figure 43-1, a service-provider domain would be larger than an operator domain and might have a maintenance level of 6, while the operator domain maintenance level is 3 or 4.

As shown in Figure 43-2, domains cannot intersect or overlap because that would require management by more than one entity, which is not allowed. Domains can touch or nest (if the outer domain has a higher maintenance level than the nested domain). Nesting domains is useful when a service provider contract with one or more operators to provide Ethernet service. Each operator has its own maintenance domain and the service provider domain is a superset of the operator domains. Maintenance levels of nesting domains should be communicated among the administrating organizations. CFM exchanges messages and performs operations on a per-domain basis.
Maintenance Associations and Maintenance Points

A maintenance association (MA) identifies a service that can be uniquely identified within the maintenance domain. The CFM protocol runs within a maintenance association. A maintenance point is a demarcation point on an interface that participates in CFM within a maintenance domain. Maintenance points drop all lower-level frames and forward all higher-level frames. There are two types of maintenance points:

- Maintenance end points (MEPs) are points at the edge of the domain that define the boundaries and confine CFM messages within these boundaries. **Outward facing or Down MEPs** communicate through the wire side (connected to the port). **Inward facing or Up MEPs** communicate through the relay function side, not the wire side.
Chapter 43  Configuring Ethernet OAM, CFM, and E-LMI

Note

CFM draft 1 referred to inward and outward-facing MEPs. CFM draft 8.1 refers to up and down MEPs, respectively. This document uses the CFM 8.1 terminology for direction.

CFM draft 1 supported only up MEPs on a per-port or per-VLAN basis. CFM 802.1ag supports up and down per-VLAN MEPs, as well as port MEPs, which are untagged down MEPs that are not associated with a VLAN. Port MEPs are configured to protect a single hop and used to monitor link state through CFM. If a port MEP is not receiving continuity check messages from its peer (static remote MEP), for a specified interval, the port is put into an operational down state in which only CFM and OAM packets pass through, and all other data and control packets are dropped.

- An up MEP sends and receives CFM frames through the relay function. It drops all CFM frames at its level or lower that come from the wire side, except traffic going to the down MEP. For CFM frames from the relay side, it processes the frames at its level and drops frames at a lower level. The MEP transparently forwards all CFM frames at a higher level, regardless of whether they are received from the relay or wire side. If the port on which MEP is configured is blocked by STP, the MEP can still send or receive CFM messages through the relay function. CFM runs at the provider maintenance level (UPE-to-UPE), specifically with up MEPs at the user network interface (UNI).

- A down MEP sends and receives CFM frames through the wire connected to the port on which the MEP is configured. It drops all CFM frames at its level or lower that come from the relay side. For CFM frames from the wire side, it processes all CFM frames at its level and drops CFM frames at lower levels except traffic going to the other lower-level down MEP. The MEP transparently forwards all CFM frames at a higher level, regardless of whether they are received from the relay or through the wire.

- Maintenance intermediate points (MIPs) are internal to a domain, not at the boundary, and respond to CFM only when triggered by traceroute and loopback messages. They forward CFM frames received from MEPs and other MIPs, drop all CFM frames at a lower level (unless MIP filtering is enabled), and forward all CFM frames at a higher level and at a lower level and regardless of whether they are received from the relay or wire side. When MIP filtering is enabled, the MIP drops CFM frames at a lower level. MIPs also catalog and forward continuity check messages (CCMs), but do not respond to them.

In the first draft of CFM, MIP filtering was always enabled. In draft 8.1, MIP filtering is disabled by default, and you can configure it to be enabled or disabled. When MIP filtering is disabled, all CFM frames are forwarded.

You can manually configure a MIP or configure the switch to automatically create a MIP. You can configure a MEP without a MIP. In case of a configuration conflict, manually created MIPs take precedence over automatically created MIPs.

If port on which the MEP is configured is blocked by Spanning-Tree Protocol (STP), the MIP can receive and might respond to CFM messages from both the wire and relay side, but cannot forward any CFM messages. This differs from CFM draft 1, where STP blocked ports could not send or receive CFM messages.
CFM Messages

CFM uses standard Ethernet frames distinguished by EtherType or (for multicast messages) by MAC address. All CFM messages are confined to a maintenance domain and to a service-provider VLAN (S-VLAN). These CFM messages are supported:

- **Continuity Check (CC) messages**—multicast heartbeat messages exchanged periodically between MEPs that allow MEPs to discover other MEPs within a domain and allow MIPs to discover MEPs. CC messages are configured to a domain or VLAN. Enter the `continuity-check` Ethernet service configuration command to enable CCM.

  The default continuity check message (CCM) interval on the switch is 10 seconds. You can set it to be 100 ms, 1 second, 1 minute, or 10 minutes by entering the `continuity-check interval` Ethernet service mode command. Because faster CCM rates are more CPU intensive, we do not recommend configuring a large number of MEPs running at 100 ms intervals.

- **Loopback messages**—unicast or multicast frames transmitted by a MEP at administrator request to verify connectivity to a particular maintenance point, indicating if a destination is reachable. A loopback message is similar to an Internet Control Message Protocol (ICMP) ping message. Refer to the `ping ethernet` privileged EXEC command.

- **Traceroute messages**—multicast frames transmitted by a MEP at administrator request to track the path (hop-by-hop) to a destination MEP. Traceroute messages are similar in concept to UDP traceroute messages. Refer to the `traceroute ethernet` privileged EXEC command.

Crosscheck Function and Static Remote MEPs

The crosscheck function is a timer-driven post-provisioning service verification between dynamically configured MEPs (using crosscheck messages) and expected MEPs (by configuration) for a service. It verifies that all endpoints of a multipoint service are operational. The crosscheck function is performed only once and is initiated from the command-line interface (CLI).

CFM 802.1ag also supports static remote MEPs or static RMEP check. Unlike the crosscheck function, which is performed only once, configured static RMEP checks run continuously. To configure static RMEP check, enter the `continuity-check static rmep` Ethernet CFM service mode command.

SNMP Traps and Fault Alarms

The MEPs generate two types of SNMP traps: CC traps and crosscheck traps. Supported CC traps are MEP up, MEP down, cross-connect (a service ID does not match the VLAN), loop, and configuration error. The crosscheck traps are service up, MEP missing (an expected MEP is down), and unknown MEP.

Fault alarms are unsolicited notifications sent to alert the system administrator when CFM detects a fault. In CFM draft 1, fault alarms were sent instantaneously when detected. In CFM 802.1ag, you can configure the priority level of alarms that trigger an SNMP trap or syslog message. You can also configure a delay period before a fault alarm is sent and the time before the alarm is reset.
Configuration Error List

CFM configuration errors in CFM 802.1ag can be misconfigurations or extra configuration commands detected during MEP configuration. They can be caused by overlapping maintenance associations. For example, if you create a maintenance association with a VLAN list and a MEP on an interface, a potential leak error could occur if other maintenance associations associated with the same VLAN exist at a higher level without any MEPs configured. You can display the configuration error list, which is informational only, by entering the `show ethernet cfm errors configuration` privileged EXEC command.

CFM Version Interoperability

When customers upgrade their network from the Cisco CFM draft 1 to IEEE standardized 802.1ag CFM, they might not upgrade all equipment at the same time, which could result in a mix of Cisco CFM draft 1 and IEEE standardized CFM devices in the network. CFM areas are regions in a network running Cisco CFM draft 1 software. Internal area bridges are all Cisco devices running CFM draft 1, and external area bridges are devices (Cisco or third-party devices) running IEEE standardized 802.1ag CFM.

Devices at the edge of these areas perform message translation. Translation is not needed for maintenance domains that do not span different areas (that is, where CFM messages end on a port on the device) since the port can respond in the same message format as was received. However, for maintenance domains that span across two areas, the device must translate the CFM message appropriately before sending it on to the other area.

When designing a network with CFM areas, follow these guidelines:

- Whenever possible, group devices with the same CFM version together.
- Minimize the number of boundaries between CFM clusters, minimizing the number of devices that must perform translation.
- Never mix CFM versions on a single segment.

When the network does use both versions of CFM, you can enable translation on the CFM 802.1ag port that is connected to the draft 1 device by entering the `ethernet cfm version cisco` interface configuration command. This command is not supported on port channels or on EtherChannel member ports.

---

**Note**

If you are running CFM draft 1 and upgrade to a software version that supports CFM 802.1ag, the switch automatically transfers the draft 1 configuration to the standard.

IP SLAs Support for CFM

The switch supports CFM with IP Service Level Agreements (SLAs), which provides the ability to gather Ethernet layer network performance metrics. Available statistical measurements for the IP SLAs CFM operation include round-trip time, jitter (interpacket delay variance), and packet loss. You can schedule multiple IP SLAs operations and use Simple Network Management Protocol (SNMP) trap notifications and syslog messages for proactive threshold violation monitoring.

For more information about IP SLAs, see Chapter 41, “Configuring Cisco IOS IP SLAs Operations.” IP SLAs integration with CFM gathers Ethernet layer statistical measurements by sending and receiving Ethernet data frames between CFM MEPs. Performance is measured between the source MEP and the destination MEP. Unlike other IP SLAs operations that provide performance metrics for only the IP layer, IP SLAs with CFM provides performance metrics for Layer 2.
You can manually configure individual Ethernet ping or jitter operations. You can also configure an IP SLAs automatic Ethernet operation that queries the CFM database for all MEPs in a given maintenance domain and VLAN. The operation then automatically creates individual Ethernet ping or jitter operations based on the discovered MEPs.

Because IP SLAs is a Cisco proprietary feature, interoperability between CFM draft 1 and CFM 802.1ag is handled automatically by the switch.

For more information about IP SLAs operation with CFM, see the IP SLAs for Metro-Ethernet feature module at this URL:


### Configuring Ethernet CFM

Configuring Ethernet CFM requires configuring the CFM domain. You can optionally configure and enable other CFM features such as crosschecking, remote MEP, port MEPs, SNMP traps, and fault alarms. Note that some of the configuration commands and procedures differ from those used in CFM draft 1.

- Default Ethernet CFM Configuration, page 43-7
- Ethernet CFM Configuration Guidelines, page 43-8
- Configuring the CFM Domain, page 43-8
- Configuring Ethernet CFM Crosscheck, page 43-12
- Configuring Static Remote MEP, page 43-13
- Configuring a Port MEP, page 43-14
- Configuring SNMP Traps, page 43-15
- Configuring Fault Alarms, page 43-16
- Configuring IP SLAs CFM Operation, page 43-17
- Configuring CFM on C-VLAN (Inner VLAN), page 43-21

### Default Ethernet CFM Configuration

CFM is globally disabled.

CFM is enabled on all interfaces when CFM is globally enabled.

A port can be configured as a flow point (MIP/MEP), a transparent port, or disabled (CFM disabled). By default, ports are transparent ports until configured as MEP, MIP, or disabled.

There are no MEPs or MIPs configured.

When configuring a MEP, if you do not configure direction, the default is up (inward facing).
Ethernet CFM Configuration Guidelines

- CFM is not supported on and cannot be configured on routed ports or on Layer 3 EtherChannels.
- CFM is supported on Layer 2 EtherChannel port channels. You can configure an EtherChannel port channel as MEP or MIP. However, CFM is not supported on individual ports that belong to an EtherChannel and you cannot add a CFM port to an EtherChannel group.
- Port MEP is not supported on Layer 2 EtherChannels, or on ports that belong to an EtherChannel.
- You cannot configure CFM on VLAN interfaces.
- CFM is supported on trunk ports, access ports, and 802.1Q tunnel ports with these exceptions:
  - Trunk ports configured as MEPs must belong to allowed VLANs
  - Access ports configured as MEPs must belong to the native VLAN.
- You cannot configure CFM on an EoMPLS port.
- You cannot configure CFM on an EoMPLS port.
- CFM is not supported on private VLAN ports.
- A REP port or FlexLink port can also be a service (VLAN) MEP or MIP, but it cannot be a port MEP.
- CFM is supported on ports running STP.
- You must configure a port MEP at a lower level than any service (VLAN) MEPs on an interface.
- An 802.1Q (QinQ) tunnel port can be a CFM up MEP or a port MEP
- A QinQ port cannot be a down MEP or a MIP; you can configure the port as a MIP, but it is not active or visible in traceroute. Port MEP frames received on a QinQ interface are not tunneled and are processed locally.
- On a QinQ port, ingress draft 1 traffic is tunneled without translation or consideration of CFM version.
- You cannot configure tunnel mode by using the native VLAN as the S-VLAN or the C-VLAN.
- For port MEP on a QinQ port, do not enter the `vlan dot1q tag native` global configuration command to enable tagging on native VLAN frames.
- Do not configure tagged or untagged 802.1ag CFM packets entering an 802.1Q tunnel port.
- Do not configure double-tagged 802.1ag CFM packets entering a trunk port.
- The Catalyst 3750 Metro switch supports CFM over pseudowire, but you cannot configure CFM on the pseudowire itself. For port-based pseudowire, CFM packets are transparently tunnelled. For VLAN-based pseudowire, you can configure CFM on the switchport (attachment circuit).

Configuring the CFM Domain

Beginning in privileged EXEC mode, follow these steps to configure the Ethernet CFM domain, configure a service to connect the domain to a VLAN, or configure a port to act as a MEP. You can also enter the optional commands to configure other parameters, such as continuity checks.

```
Note
You do not need to enter the `ethernet cfm ieee` global configuration command to configure the CFM version as IEEE 802.1ag. If you are running Cisco IOS Release 12.2(52)SE or later, the CFM version is always 802.1ag and the command is automatically generated when you enable CFM.
```
### Configuring Ethernet CFM

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>ethernet cfm global</code></td>
<td>Globally enable Ethernet CFM on the switch.</td>
</tr>
<tr>
<td>Step 3</td>
<td>`ethernet cfm traceroute cache [size entries</td>
<td>(Optional) Configure the CFM traceroute cache. You can set a maximum cache size or hold time.</td>
</tr>
<tr>
<td></td>
<td>hold-time minutes]</td>
<td>• (Optional) For <code>size</code>, enter the cache size in number of entry lines. The range is from 1 to 4095; the default is 100 lines.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) For <code>hold-time</code>, enter the maximum cache hold time in minutes. The range is from 1 to 65535; the default is 100 minutes.</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>ethernet cfm mip auto-create level level-id</code></td>
<td>(Optional) Configure the switch to automatically create MIPs for VLAN IDS that are not associated with specific maintenance associations at the specified level. The level range is 0 to 7.</td>
</tr>
<tr>
<td></td>
<td><code>vlan vlan-id</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> Configure MIP auto-creation only for VLANs that MIPs should monitor. Configuring for all VLANs can be CPU and memory-intensive.</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>ethernet cfm mip filter</code></td>
<td>(Optional) Enable MIP filtering, which means that all CFM frames at a lower level are dropped. The default is disabled.</td>
</tr>
<tr>
<td>Step 6</td>
<td><code>ethernet cfm domain domain-name level level-id</code></td>
<td>Define a CFM domain, set the domain level, and enter ethernet-cfm configuration mode for the domain. The maintenance level number range is 0 to 7.</td>
</tr>
<tr>
<td>Step 7</td>
<td>`id {mac-address domain_number</td>
<td>dns name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>mac-address domain_number</code>—Enter the MAC address and a domain number. The number can be from 0 to 65535.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>dns name</code>—Enter a DNS name string. The name can be a maximum of 43 characters.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>null</code>—Assign no domain name.</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Purpose</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| 8    | service {ma-name | ma-number | vpn-id vpn} {vlan vlan-id [direction down] | port} | Define a customer service maintenance association (MA) name or number or VPN ID to be associated with the domain, a VLAN ID or port MEP, and enter ethernet-cfm-service configuration mode.  
  - ma-name—a string of no more than 100 characters that identifies the MAID.  
  - ma-number—a value from 0 to 65535.  
  - vpn-id vpn—enter a VPN ID as the ma-name.  
  - vlan vlan-id—VLAN range is from 1 to 4094. You cannot use the same VLAN ID for more than one domain at the same level.  
  - (Optional) direction down—specify the service direction as down.  
  - port—Configure port MEP, a down MEP that is untagged and not associated with a VLAN. |
| 9    | continuity-check | Enable sending and receiving of continuity check messages. |
| 10   | continuity-check interval value | (Optional) Set the interval at which continuity check messages are sent. The available values are 100 ms, 1 second, 10 seconds, 1 minute and 10 minutes. The default is 10 seconds.  
  **Note** Because faster CCM rates are more CPU-intensive, we do not recommend configuring a large number of MEPs running at 100 ms intervals. |
| 11   | continuity-check loss-threshold threshold-value | (Optional) Set the number of continuity check messages to be missed before declaring that an MEP is down. The range is 2 to 255; the default is 3. |
| 12   | maximum meps value | (Optional) Configure the maximum number of MEPs allowed across the network. The range is from 1 to 65535. The default is 100. |
| 13   | sender-id {chassis | none} | (Optional) Include the sender ID TLVs, attributes containing type, length, and values for neighbor devices.  
  - chassis—Send the chassis ID (host name).  
  - none—Do not include information in the sender ID. |
| 14   | mip auto-create [lower-mep-only | none] | (Optional) Configure auto creation of MIPs for the service.  
  - lower-mep-only—Create a MIP only if there is a MEP for the service in another domain at the next lower active level.  
  - none—No MIP auto-create. |
| 15   | exit | Return to ethernet-cfm configuration mode. |
# Configuring Ethernet CFM

**Purpose**  (Optional) Configure auto creation of MIPs for the domain.
- **lower-mep-only**—Create a MIP only if there is a MEP for the service in another domain at the next lower active level.

**Purpose**  (Optional) Set the number of minutes that data from a missing maintenance end point is kept before it is purged. The range is 1 to 65535; the default is 100 minutes.

**Purpose**  Return to global configuration mode.

**Purpose**  Specify an interface to configure, and enter interface configuration mode.

**Purpose**  (Optional) Configure the port as a trunk port.

**Purpose**  (Optional) Configure a customer level or service-provider level maintenance intermediate point (MIP) for the interface. The MIP level range is 0 to 7.

**Note**  This step is not required if you have entered the `ethernet cfm mip auto-create` global configuration command or the `mip auto-create` ethernet-cfm or ethernet-cfm-srv configuration mode.

**Purpose**  Configure maintenance end points for the domain, and enter ethernet cfm mep mode.
- **domain domain-name**—Specify the name of the created domain.
- **mpid identifier**—Enter a maintenance end point identifier. The identifier must be unique for each VLAN (service instance). The range is 1 to 8191.
- **vlan vlan-id**—Enter the service provider VLAN ID or IDs as a VLAN-ID (1 to 4094), a range of VLAN-IDs separated by a hyphen, or a series of VLAN IDs separated by comma.
- **port**—Configure port MEP.

**Purpose**  (Optional) Specify the class of service (CoS) value to be sent with the messages. The range is 0 to 7.

**Purpose**  Return to privileged EXEC mode.

**Purpose**  Verify the configuration.

**Purpose**  (Optional) Display the configuration error list.

**Purpose**  (Optional) Save your entries in the configuration file.

Use the no versions of the commands to remove the configuration or return to the default configurations.

This is an example of the basic CFM configuration:

```
Switch(config)# ethernet cfm ieee
Switch(config)# ethernet cfm global
Switch(config)# ethernet cfm domain abc level 3
```
Configuring Ethernet CFM Crosscheck

Beginning in privileged EXEC mode, follow these steps to configure Ethernet CFM crosscheck:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>ethernet cfm mep crosscheck start-delay delay</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>ethernet cfm domain domain-name level level-id</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>service {ma-name</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>mep mpid identifier</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>ethernet cfm mep crosscheck {enable</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>show ethernet cfm maintenance-points remote crosscheck</td>
</tr>
</tbody>
</table>
Configuring Ethernet CFM

Use the no form of each command to remove a configuration or to return to the default settings.

### Configuring Static Remote MEP

Beginning in privileged EXEC mode, follow these steps to configure Ethernet CFM static remote MEP:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>ethernet cfm domain domain-name level level-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>service {ma-name | ma-number | vpn-id vpn} | vlan vlan-id | direction down | port}</td>
</tr>
<tr>
<td></td>
<td>• ma-name—a string of no more than 100 characters that identifies the MAID.</td>
</tr>
<tr>
<td></td>
<td>• ma-number—a value from 0 to 65535.</td>
</tr>
<tr>
<td></td>
<td>• vpn-id—enter a VPN ID as the ma-name.</td>
</tr>
<tr>
<td></td>
<td>• vlan vlan-id—VLAN range is from 1 to 4094. You cannot use the same VLAN ID for more than one domain at the same level.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) direction down—specify the service direction as down.</td>
</tr>
<tr>
<td></td>
<td>• port—Configure port MEP, a down MEP that is untagged and not associated with a VLAN.</td>
</tr>
<tr>
<td>Step 4</td>
<td>continuity-check</td>
</tr>
<tr>
<td>Step 5</td>
<td>mep mpid identifier</td>
</tr>
<tr>
<td>Step 6</td>
<td>continuity-check static rmp</td>
</tr>
<tr>
<td>Step 7</td>
<td>end</td>
</tr>
<tr>
<td>Step 8</td>
<td>show ethernet cfm maintenance-points remote static</td>
</tr>
</tbody>
</table>
Chapter 43 Configuring Ethernet OAM, CFM, and E-LMI

Configuring Ethernet CFM

Use the `no` form of each command to remove a configuration or to return to the default settings.

### Configuring a Port MEP

A port MEP is a down MEP that is not associated with a VLAN and that uses untagged frames to carry CFM messages. You configure port MEPs on two connected interfaces. Port MEPs are always configured at a lower domain level than native VLAN MEPs.

Beginning in privileged EXEC mode, follow these steps to configure Ethernet CFM port MEPs:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code> Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>ethernet cfm domain domain-name level level-id</code> Define a CFM domain, set the domain level, and enter ethernet-cfm configuration mode for the domain. The maintenance level number range is 0 to 7.</td>
</tr>
<tr>
<td>Step 3</td>
<td>`service {ma-name</td>
</tr>
<tr>
<td></td>
<td>• <code>ma-name</code>—a string of no more than 100 characters that identifies the MAID.</td>
</tr>
<tr>
<td></td>
<td>• <code>ma-number</code>—a value from 0 to 65535.</td>
</tr>
<tr>
<td></td>
<td>• <code>vpn-id vpn</code>—enter a VPN ID as the <code>ma-name</code>.</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>mep mpid identifier</code> Define the static remote maintenance end point identifier in the domain and service. The range is 1 to 8191.</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>continuity-check</code> Enable sending and receiving of continuity check messages.</td>
</tr>
<tr>
<td>Step 6</td>
<td><code>continuity-check interval value</code> (Optional) Set the interval at which continuity check messages are sent. The available values are 100 ms, 1 second, 10 seconds, 1 minute and 10 minutes. The default is 10 seconds.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Because faster CCM rates are more CPU-intensive, we do not recommend configuring a large number of MEPs running at 100 ms intervals.</td>
</tr>
<tr>
<td>Step 7</td>
<td><code>continuity-check loss-threshold threshold-value</code> (Optional) Set the number of continuity check messages to be missed before declaring that an MEP is down. The range is 2 to 255; the default is 3.</td>
</tr>
</tbody>
</table>
Chapter 43  Configuring Ethernet OAM, CFM, and E-LMI

Configuring Ethernet CFM

### Configuring Ethernet CFM

Use the `no` form of each command to remove a configuration or to return to the default settings.

This is a sample configuration for a port MEP:

```
Switch(config)# ethernet cfm domain abc level 3
Switch(config-ecfm)# service PORTMEP port
Switch(config-ecfm-srv)# mep mpid 222
Switch(config-ecfm-srv)# continuity-check
Switch(config-ecfm-srv)# continuity-check static rmep
Switch(config-ecfm-srv)# exit
Switch(config-ecfm)# exit
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ethernet cfm mep domain abc mpid 111 port
```

### Configuring SNMP Traps

Beginning in privileged EXEC mode, follow these steps to configure traps for Ethernet CFM:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>snmp-server enable traps ethernet cfm cc [mep-up] [mep-down] [config] [loop] [cross-connect]</td>
<td>(Optional) Enable Ethernet CFM continuity check traps.</td>
</tr>
<tr>
<td>snmp-server enable traps ethernet cfm crosscheck [mep-unknown] [mep-missing] [service-up]</td>
<td>(Optional) Enable Ethernet CFM crosscheck traps.</td>
</tr>
</tbody>
</table>

Use the `no` form of each command to remove a configuration or to return to the default settings.

Step 8  `continuity-check static rmep`  Enable checking of the incoming continuity check message from a remote MEP that is configured in the MEP list.

Step 9  `exit`  Return to ethernet-cfm configuration mode.

Step 10 `exit`  Return to global configuration mode.

Step 11 `interface interface-id`  Identify the port MEP interface and enter interface configuration mode.

Step 12 `ethernet cfm mep domain domain-name mpid identifier port`  Configure the interface as a port MEP for the domain.

- **domain domain-name**—Specify the name of the created domain.

- **mpid identifier**—Enter a maintenance end point identifier. The identifier must be unique for each VLAN (service instance). The range is 1 to 8191.

Step 13 `end`  Return to privileged EXEC mode.

Step 14 `show ethernet cfm maintenance-points remote static`  Verify the configuration.

Step 15 `show ethernet cfm errors [configuration]`  Enter this command after you enable CFM crosscheck to display the results of the crosscheck operation. Enter the `configuration` keyword to display the configuration error list.

Step 16 `copy running-config startup-config`  (Optional) Save your entries in the configuration file.
Configuring Fault Alarms

Beginning in privileged EXEC mode, follow these steps to configure Ethernet CFM fault alarms. Note that you can configure fault alarms in either global configuration mode or Ethernet CFM interface MEP mode. In case of conflict, the interface MEP mode configuration takes precedence.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4</td>
<td><strong>end</strong></td>
</tr>
<tr>
<td>Step 5</td>
<td><strong>show running-config</strong></td>
</tr>
<tr>
<td>Step 6</td>
<td><strong>copy running-config startup-config</strong></td>
</tr>
</tbody>
</table>

Use the **no** form of each command to remove a configuration or to return to the default settings.

### Configuring Fault Alarms

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td>Step 2</td>
<td><strong>ethernet cfm alarm notification</strong></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><strong>ethernet cfm alarm delay</strong></td>
</tr>
<tr>
<td>Step 4</td>
<td><strong>ethernet cfm alarm reset</strong></td>
</tr>
<tr>
<td>Step 5</td>
<td><strong>ethernet cfm logging alarm ieee</strong></td>
</tr>
<tr>
<td>Step 6</td>
<td><strong>interface</strong></td>
</tr>
</tbody>
</table>
Chapter 43  Configuring Ethernet OAM, CFM, and E-LMI

Configuring Ethernet CFM

Use the no form of each command to remove a configuration or to return to the default settings.

**Configuring IP SLAs CFM Operation**

You can manually configure an individual IP SLAs Ethernet ping or jitter echo operation or you can configure IP SLAs Ethernet operation with endpoint discovery. You can also configure multiple operation scheduling. For accurate one-way delay statistics, the clocks on the endpoint switches must be synchronized. You can configure the endpoint switches with Network Time Protocol (NTP) so that the switches are synchronized to the same clock source.

### Step 7

```
ethernet cfm mep domain domain-name mpid domain-name identifier vlan vlan-id
```

Configure maintenance end points for the domain, and enter ethernet cfm interface mep mode.

- **domain domain-name**—Specify the name of the created domain.
- **mpid identifier**—Enter a maintenance end point identifier. The identifier must be unique for each VLAN (service instance). The range is 1 to 8191.
- **vlan vlan-id**—Enter the service provider VLAN ID or IDs as a VLAN-ID (1 to 4094), a range of VLAN-IDs separated by a hyphen, or a series of VLAN IDs separated by comma.

### Step 8

```
ethernet cfm alarm notification { all | error-xcon | mac-remote-error-xcon | none | remote-error-xcon | xcon }
```

(Optional) Enable Ethernet CFM fault alarm notification for the specified defects on the interface.

**Note**  
The Ethernet CFM interface MEP alarm configuration takes precedence over the global configuration.

### Step 9

```
ethernet cfm alarm { delay value | reset value }
```

(Optional) Set an alarm delay period or a reset period.

**Note**  
The Ethernet CFM interface MEP alarm configuration takes precedence over the global configuration.

### Step 10

```
end
```

Return to privileged EXEC mode.

### Step 11

```
show running-config
```

Verify your entries.

### Step 12

```
copy running-config startup-config
```

(Optional) Save your entries in the configuration file.

For detailed information about configuring IP SLAs operations, see the *Cisco IOS IP SLAs Configuration Guide, Release 12.4T* at this URL:


For detailed information about IP SLAs commands, see the command reference at this URL:

This section includes these procedures:

- Manually Configuring an IP SLAs CFM Probe or Jitter Operation, page 43-18
- Configuring an IP SLAs Operation with Endpoint Discovery, page 43-20

**Manually Configuring an IP SLAs CFM Probe or Jitter Operation**

Beginning in privileged EXEC mode, follow these steps to manually configure an IP SLAs Ethernet echo (ping) or jitter operation:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>ip sla operation-number</td>
</tr>
<tr>
<td></td>
<td>Create an IP SLAs operation, and enter IP SLAs configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>ethernet echo mpid identifier domain domain-name vlan vlan-id</td>
</tr>
<tr>
<td></td>
<td>Configure the IP SLAs operation as an echo (ping) or jitter operation, and enter IP SLAs Ethernet echo configuration mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter echo for a ping operation or jitter for a jitter operation.</td>
</tr>
<tr>
<td></td>
<td>• For mpid identifier, enter a maintenance endpoint identifier. The identifier must be unique for each VLAN (service instance). The range is 1 to 8191.</td>
</tr>
<tr>
<td></td>
<td>• For domain domain-name, enter the CFM domain name.</td>
</tr>
<tr>
<td></td>
<td>• For vlan vlan-id, the VLAN range is from 1 to 4095.</td>
</tr>
<tr>
<td></td>
<td>• (Optional—for jitter only) Enter the interval between sending of jitter packets.</td>
</tr>
<tr>
<td></td>
<td>• (Optional—for jitter only) Enter the num-frames and the number of frames to be sent.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>cos cos-value</td>
</tr>
<tr>
<td></td>
<td>(Optional) Set a class of service value for the operation. Before configuring the cos parameter on the Catalyst 3750 Metro switch, you must globally enable QoS by entering the mls qos global configuration command.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>frequency seconds</td>
</tr>
<tr>
<td></td>
<td>(Optional) Set the rate at which the IP SLAs operation repeats. The range is from 1 to 604800 seconds; the default is 60 seconds.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>history history-parameter</td>
</tr>
<tr>
<td></td>
<td>(Optional) Specify parameters for gathering statistical history information for the IP SLAs operation.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>owner owner-id</td>
</tr>
<tr>
<td></td>
<td>(Optional) Configure the SNMP owner of the IP SLAs operation.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>request-data-size bytes</td>
</tr>
<tr>
<td></td>
<td>(Optional) Specify the protocol data size for an IP SLAs request packet. The range is from 0 to the maximum size allowed by the protocol being used; the default is 66 bytes.</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>tag text</td>
</tr>
<tr>
<td></td>
<td>(Optional) Create a user-specified identifier for an IP SLAs operation.</td>
</tr>
</tbody>
</table>
### Chapter 43 Configuring Ethernet OAM, CFM, and E-LMI

#### Configuring Ethernet CFM

**Step 10**

```
threshold milliseconds
```

(Optional) Specify the upper threshold value in milliseconds (ms) for calculating network monitoring statistics. The range is 0 to 2147483647; the default is 5000.

**Step 11**

```
timeout milliseconds
```

(Optional) Specify the amount of time in ms that the IP SLAs operation waits for a response from its request packet. The range is 0 to 604800000; the default value is 5000.

**Step 12**

```
exit
```

Return to global configuration mode.

**Step 13**

```
ip sla schedule operation-number [ageout seconds] [life {forever | seconds}] [recurring] [start-time {hh:mm:ss | month day | day month | pending | now | after hh:mm:ss}]
```

Schedule the time parameters for the IP SLAs operation.

- **operation-number**—Enter the IP SLAs operation number.
- (Optional) **ageout seconds**—Enter the number of seconds to keep the operation in memory when it is not actively collecting information. The range is 0 to 2073600 seconds. The default is 0 seconds.
- (Optional) **life**—Set the operation to run indefinitely (forever) or for a specific number of seconds. The range is from 0 to 2147483647. The default is 3600 seconds (1 hour)
- (Optional) **recurring**—Set the probe to be automatically scheduled every day.
- (Optional) **start-time**—Enter the time for the operation to begin collecting information:
  - To start at a specific time, enter the hour, minute, second (in 24-hour notation), and day of the month.
  - Enter **pending** to select no information collection until a start time is selected.
  - Enter **now** to start the operation immediately.
  - Enter after **hh:mm:ss** to show that the operation should start after the entered time has elapsed.

**Step 14**

```
end
```

Return to privileged EXEC mode.

**Step 15**

```
show ip sla configuration [operation-number]
```

Show the configured IP SLAs operation.

**Step 16**

```
copy running-config startup-config
```

(Optional) Save your entries in the configuration file.

To remove an IP SLAs operation, enter the no **ip sla operation-number** global configuration command.
Configuring an IP SLAs Operation with Endpoint Discovery

Beginning in privileged EXEC mode, follow these steps to use IP SLAs to automatically discover the CFM endpoints for a domain and VLAN ID. You can configure ping or jitter operations to the discovered endpoints.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip sla ethernet-monitor operation-number</td>
</tr>
<tr>
<td>Step 3</td>
<td>type echo domain domain-name vlan vlan-id [exclude-mpids mp-ids] or type jitter domain domain-name vlan vlan-id [exclude-mpids mp-ids] [interval interpacket-interval] [num-frames number-of frames transmitted]</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>cos cos-value</td>
</tr>
<tr>
<td>Step 5</td>
<td>owner owner-id</td>
</tr>
<tr>
<td>Step 6</td>
<td>request-data-size bytes</td>
</tr>
<tr>
<td>Step 7</td>
<td>tag text</td>
</tr>
<tr>
<td>Step 8</td>
<td>threshold milliseconds</td>
</tr>
<tr>
<td>Step 9</td>
<td>timeout milliseconds</td>
</tr>
</tbody>
</table>
Configuring Ethernet CFM

Step 10

exit

Return to global configuration mode.

Step 11

ip sla schedule operation-number [ageout seconds] [life {forever | seconds}] [recurring] [start-time {hh:mm:ss} [month day | day month] | pending | now | after hh:mm:ss]

Schedule the time parameters for the IP SLAs operation.

- operation-number—Enter the IP SLAs operation number.
- (Optional) ageout seconds—Enter the number of seconds to keep the operation in memory when it is not actively collecting information. The range is 0 to 2073600 seconds. The default is 0 seconds.
- (Optional) life—Set the operation to run indefinitely (forever) or for a specific number of seconds. The range is from 0 to 2147483647. The default is 3600 seconds (1 hour)
- (Optional) recurring—Set the probe to be automatically scheduled every day.
- (Optional) start-time—Enter the time for the operation to begin collecting information:
  - To start at a specific time, enter the hour, minute, second (in 24-hour notation), and day of the month.
  - Enter pending to select no information collection until a start time is selected.
  - Enter now to start the operation immediately.
  - Enter after hh:mm:ss to show that the operation should start after the entered time has elapsed.

Step 12

del

Return to privileged EXEC mode.

Step 13

show ip sla configuration [operation-number]

Show the configured IP SLAs operation.

Step 14

copy running-config startup-config

(Optional) Save your entries in the configuration file.

To remove an IP SLAs operation, enter the no ip sla operation-number global configuration command.

Configuring CFM on C-VLAN (Inner VLAN)

The implementation of IEEE 802.1ag CFM prior to Cisco IOS Release 12.2(54)SE allows provisioning of maintenance points on the S-VLAN component. It does not allow monitoring or troubleshooting when QinQ is enabled on the provider-edge (PE) device. Cisco IOS Release 12.2(54)SE and later allow customers to provision maintenance intermediate points (MIPs) and Up maintenance endpoints (MEPs) on the C-VLAN (inner VLAN) component of QinQ or 802.1ad ports to provide visibility on the C-VLAN. In addition, some C-VLAN restrictions are removed and C-VLANs are now supported on 802.1q tunnel ports.

For more information about this feature and the supported commands, see:

The switch supports 802.1q-tunnel-port mode
Feature Support and Behavior

CFM S-VLAN component support:

- Up MEPs at any level (0 to 7).
  
  Up MEPs use the port access VLAN ID (the outer tag or S-VLAN).

  CFM frames sent and received by Up MEPs have a single VLAN tag, and the VLAN identifier is the
  port access VLAN ID (S-VLAN). Because the 802.1q tunnel interface marks the endpoint of the
  S-VLAN, the associated S-VLAN component should mark the endpoint of the CFM domain running
  over the S-VLAN space.

CFM C-VLAN component support:

- Up MEP functions at any level (0 to 7).
  
  Up MEPs use two tags: an outer tag with a VLAN ID that is the port access VLAN (S-VLAN) and
  an inner tag with a selected C-VLAN that is allowed through the 802.1q tunnel port. CFM frames
  sent and received by these Up MEPs are always double-tagged.

- MIP functions at any level (0 to 7).
  
  MIPs process CFM frames that are single-tagged when coming from the wire-side and
double-tagged when coming from the relay-function side.

- Transparent point functions.

Port MEP frames are always sent untagged, even when the `dot1q vlan native` tag is enabled.

Supported maintenance points on 802.1q tunnels:

- Up MEP on the C-VLAN component for selective or all-to-one bundling
- Up MEP on the S-VLAN
- Port MEP
- MIP support on C-VLAN component for selective or all-to-one bundling

Note: The switch supports only manual configuration of MIPs. It does not support MIP autocreation on
C-VLANs.

Platform Restrictions and Limitations

- Maximum supported MEPs per switch at each continuity check message (CCM) interval:
  
  - 1600 MEP local and 1600 MEP remote (on C-VLAN and S-VLAN) with 10-second intervals
  - 250 MEP local and 250 MEP remote (on C-VLAN and S-VLAN) with 1-second intervals
  - 30 MEP local and 30 MEP remote (on C-VLAN and S-VLAN) with 100-ms intervals

- Maximum supported MIPs at each CCM interval:
  
  - 300 MIPs at 10 seconds
  - 125 MIPs at 1 second
  - 30 MIPs at 100 ms

- There could be issues detecting cross-connect errors on Catalyst 3750 Metro switches.
- These features are not supported:
  
  - CFM C-component on the native VLAN
Chapter 43      Configuring Ethernet OAM, CFM, and E-LMI

Understanding CFM ITU-T Y.1731 Fault Management

The ITU-T Y.1731 feature provides new CFM functionality for fault and performance management for service providers in large networks. The switch supports Ethernet Alarm Indication Signal (ETH-AIS), Ethernet Remote Defect Indication (ETH-RDI), Ethernet Locked Signal (ETH-LCK), and Ethernet Multicast Loopback Message (MCAST-LBM) functionality for fault detection, verification, and isolation.

- Port-based and VLAN-based MPLS (pseudowire) on the C-VLAN
- Down MEP on S or C-VLAN (provider network port)
- MIP on S-VLAN (provider network port)
- CFM C-VLAN alarm indication signal (AIS)
- CFM C-VLAN locked signal (LCK)
- 802.3ah interworking with CFM C-VLAN
- CFM C-VLAN IP SLAs
- CFM C-VLAN E-LMI
- CFM C-VLAN MIP autocreation.

Y.1731 Terminology

- Server MEP—the combination of the server layer termination function and server or Ethernet adaptation layer termination function or server or Ethernet adaptation function, where the server layer termination function is expected to run OAM mechanisms specific to the server layer. The supported mechanisms are link up, link down, and 802.3ah.
- Server layer—a virtual MEP layer capable of detecting fault conditions.
- Defect conditions:
  - Loss of continuity (LOC): the MEP stopped receiving CCM frames from a peer MEP
  - Mismerge: the MEP received a CCM frame with a correct maintenance level (matching the MEP level) but an incorrect maintenance ID.
  - Unexpected MEP: the MEP received a CCM frame with the correct maintenance level (matching the MEP's level) and correct maintenance ID, but an unexpected MEP ID.
  - Unexpected maintenance level: the MEP received a CCM frame with an incorrect maintenance level.
  - Unexpected period: the MEP received a CCM frame with a correct maintenance level, a correct maintenance ID, a correct MEP ID, but a different transmission period field.
- Signal fail—the MEP declares a signal fail condition when it detects a defect condition.
• Alarm Indication Signal (AIS) condition—the MEP received an AIS frame.
• Remote Defect Indication (RDI) condition—The MEP received a CCM frame with the RDI field set.
• Locked Signal (LCK) condition—The MEP received an LCK frame.

**Alarm Indication Signals**

The Ethernet Alarm Signal function (ETH-AIS) is used to suppress alarms after defects are detected at the server (sub) layer, which is a virtual MEP layer capable of detecting fault conditions. A fault condition could be a signal fail condition, an AIS condition, or a LCK condition.

Note

Although the configuration is allowed, you should not configure AIS in networks running STP. An STP configuration might cause AIS interruption or redirection.

When a MEP or a service MEP (SMEP) detects a connectivity fault at a specific maintenance association level, it multicasts AIS frames in the direction away from the detected failure at the client maintenance association level. The frequency of AIS frame transmission is based on the AIS transmission period. The first AIS frame is always sent immediately following the detection of the defect condition. We recommend a transition period of 1 second in a network of only a few VLANs to ensure that the first AIS frame is sent immediately following error detection. We recommend a 60-second interval in a network of multiple (up to 4094) VLANs to prevent stressing the network with 1-second transmissions.

A MEP that receives a frame with ETH-AIS information cannot determine the specific server with the defect condition or the set of peer MEPs for which it should suppress alarms. Therefore, it suppresses alarms for all peer MEPs, whether or not they are connected.

When a MEP receives an AIS frame, it examines it to be sure that the Maintenance Entity Group (MEG) level matches its own MEG and then detects the AIS default condition. (A MEG is Y.1731 terminology for maintenance association in 802.1ag.) After this detection, if no AIS frames are received for an interval of 3.5 times the AIS transmission period, the MEP clears the AIS defect condition. For example, if the AIS timer is set for 60 seconds, the AIS timer period expires after 3.5 times 60, or 210 seconds.

The AIS condition is terminated when a valid CCM is received with all error conditions cleared or when the AIS period timer expires (the default time is 60 seconds).

**Ethernet Remote Defect Indication**

When Ethernet OAM continuity check (ETH-CC) transmission is enabled, the Ethernet Remote Defect Indication (ETH-RDI) function uses a bit in the CFM CC message to communicate defect conditions to the MEP peers. For ETH-RDI functionality, you must configure the MEP MEG level, the ETH-CC transmission period, and the ETH-CC frame priority. ETH-RDI does not require any MIP configuration.

When a MEP receives frames with ETH-RDI information, it determines that its peer MEP has encountered a defect condition and sets the RDI files in the CCM frames for the duration of the defect condition. When the defect condition clears, the MEP clears the RDI field.

When a MEP receives a CCM frame, it examines it to ensure that its MEG level is the same and if the RDI field is set, it detects an RDI condition. For point-to-point Ethernet connections, a MEP can clear the RDI condition when it receives the first frame from its peer MEP with the RDI field cleared. However, for multipoint Ethernet connectivity, the MEP cannot determine the associated subset of peer MEPs with which the sending MEP has seen the defect condition. It can clear the RDI condition after it receives CCM frames with the RDI field cleared from its entire list of peer MEPs.
Ethernet Locked Signal

The Ethernet Locked Signal (ETH-LCK) function communicates the administrative locking of a server MEP and interruption of data traffic being forwarded to the MEP expecting the traffic. A MEP that receives frames with ETH-LCK information can differentiate between a defect condition and an administrative locking. ETH-LCK relies on loopback information (local and remote). The default timer for ETH-LCK is 60 seconds and the default level is the MIP level.

When a MEP is administratively locked, it sends LCK frames in a direction opposite to its peer MEPs, based on the LCK transmission period, which is the same as the AIS transmission period. The first LCK frame is sent immediately following the administrative or diagnostic action.

A MEP receiving a LCK frame verifies that the maintenance level matches its configured maintenance level, and detects a LCK condition. When no LCK frames are received for an interval of 3.5 times the LCK transmission period, the MEP clears the LCK condition.

Multicast Ethernet Loopback

The multicast Ethernet loopback (ETH-LB) function verifies bidirectional connectivity of a MEP with its peer MEPs and is an on-demand OAM function. When the feature is invoked on a MEP by entering the ping privileged EXEC command, the MEP sends a multicast frame with ETH-LB request information to peer MEPs in the same MEG. The MEP expects to receive a unicast frame with ETH-LB reply information from its peer MEPs within a specified time period. A MEP receiving a multicast frame with ETH-LB request information validates the frame and transmits a frame with reply information.

To configure multicast ETH-LB, you configure the MEG level of the MEP and the priority of the multicast frames with ETH-LB requests. Multicast frames with ETH-LB request information are always marked as drop ineligible. No MIP configuration is required.

The MEP sends multicast LB message frames on an on-demand basis. After sending a multicast LBM frame, the MEP expects to receive LB reply frames within 5 seconds.

When a MEP receives a valid LBM frame, it generates an LB reply frame and sends it to the requested MEP after a random delay in the range of 0 to 1 second. The validity of the frame is determined on its having the correct MEG level.

When a MEP sends a multicast LBM frame and receives an LB reply frame within 5 seconds, the LB reply frame is valid.

Configuring Y.1731 Fault Management

To configure Y.1731 fault management, you must enable CFM and configure MIPs on the participating interfaces. AIS messages are generated only on interfaces with a configured MIP.

- Default Y.1731 Configuration, page 43-25
- Configuring ETH-AIS, page 43-26
- Configuring ETH-LCK, page 43-27
- Using Multicast Ethernet Loopback, page 43-30

Default Y.1731 Configuration

ETH-AIS and ETH-LCK are enabled by default when CFM is enabled.
When you configure ETH-AIS or ETH-LCK, you must configure CFM before ETH-AIS or ETH-LCK is operational.

ETH-RDI is set automatically when continuity check messages are enabled.

## Configuring ETH-AIS

Beginning in privileged EXEC mode, follow these steps to configure Ethernet AIS on a switch:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>ethernet cfm ais link-status global</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>level level-id</td>
</tr>
<tr>
<td>or</td>
<td>disable</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>period value</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>exit</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>ethernet cfm domain domain-name level level-id</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>service {ma-name</td>
</tr>
<tr>
<td></td>
<td>• ma-name—a string of no more than 100 characters that identifies the MAID.</td>
</tr>
<tr>
<td></td>
<td>• ma-number—a value from 0 to 65535.</td>
</tr>
<tr>
<td></td>
<td>• vpn-id—enter a VPN ID as the ma-name.</td>
</tr>
<tr>
<td></td>
<td>• vlan vlan-id—VLAN range is from 1 to 4094. You cannot use the same VLAN ID for more than one domain at the same level.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) direction down—specify the service direction as down.</td>
</tr>
<tr>
<td></td>
<td>• port—Configure port MEP, a down MEP that is untagged and not associated with a VLAN.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>ais level level-id</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>ais period value</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>ais expiry-threshold value</td>
</tr>
</tbody>
</table>
Configuring Y.1731 Fault Management

Use the **no** form of the commands to return to the default configuration or to remove a configuration. To disable the generation of ETH-AIS frames, enter the **disable** config-ais-link-cfm mode command.

This is an example of the output from the **show ethernet cfm smep** command when Ethernet AIS has been enabled:

```
Switch# show ethernet cfm smep
SMEP Settings:---------------------------
Interface: GigabitEthernet1/0/3
LCK-Status: Enabled
LCK Period: 60000 (ms)
Level to transmit LCK: Default
AIS-Status: Enabled
AIS Period: 60000 (ms)
Level to transmit AIS: Default
Defect Condition: AIS
```

### Configuring ETH-LCK

Beginning in privileged EXEC mode, follow these steps to configure Ethernet locked signal on a switch:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> ethernet cfm lck link-status global</td>
<td>Configure SMEP LCK commands by entering config-lck-link-cfm mode.</td>
</tr>
</tbody>
</table>
### Command | Purpose
--- | ---
**Step 3**

| level level-id | Configure the maintenance level for sending ETH-LCK frames transmitted by the SMEP. The range is 0 to 7.  
| or | Disable generation of ETH-LCK frames. |

**Step 4**

| period value | Configure the SMEP ETH-LCK frame transmission period interval. Allowable values are 1 second or 60 seconds. |

**Step 5**

| exit | Return to global configuration mode. |

**Step 6**

| ethernet cfm domain domain-name level level-id | Define a CFM domain, set the domain level, and enter ethernet-cfm configuration mode for the domain. The maintenance level number range is 0 to 7. |

**Step 7**

| service {ma-name | ma-number | vpn-id vpn} {vlan vlan-id [direction down] | port} | Define a customer service maintenance association name or number to be associated with the domain, or a VLAN ID or VPN-ID, and enter ethernet-cfm-service configuration mode.  
| | - **ma-name**—a string of no more than 100 characters that identifies the MAID.  
| | - **ma-number**—a value from 0 to 65535.  
| | - **vpn-id**—enter a VPN ID as the **ma-name**.  
| | - **vlan vlan-id**—VLAN range is from 1 to 4094. You cannot use the same VLAN ID for more than one domain at the same level.  
| | - (Optional) **direction down**—specify the service direction as down.  
| | - **port**—Configure port MEP, a down MEP that is untagged and not associated with a VLAN. |

**Step 8**

| lck level level-id | (Optional) Configure the maintenance level for sending ETH-LCK frames sent by the MEP. The range is 0 to 7. |

**Step 9**

| lck period value | (Optional) Configure the MEP ETH-LCK frame transmission period interval. Allowable values are 1 second or 60 seconds. |

**Step 10**

| lck expiry-threshold value | (Optional) Set the expiring threshold for the MA. The range is 2 to 255. The default is 3.5. |

**Step 11**

| exit | Return to ethernet-cfm configuration mode. |

**Step 12**

| exit | Return to global configuration mode. |

**Step 13**

| interface interface-id | Specify an interface ID, and enter interface configuration mode. |

**Step 14**

| [no] ethernet cfm lck link-status | Enable or disable sending ETH-LCK frames from the SMEP on the interface. |

**Step 15**

| ethernet cfm lck link-status period value | Configure the ETH-LCK transmission period generated by the SMEP on the interface. Allowable values are 1 second or 60 seconds. |
### Command Purpose

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td><code>ethernet cfm lck link-status level level-id</code></td>
<td>Configure the maintenance level for sending ETH-LCK frames sent by the SMEP on the interface. The range is 0 to 7.</td>
</tr>
<tr>
<td>17</td>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>18</td>
<td><code>ethernet cfm lck start mpid local-mpid domain domain-name vlan vlan-id [drop l2-bpdu]</code></td>
<td>(Optional) Put a MEP in LCK condition.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The <code>mpid local-mpid domain domain-name vlan vlan-id</code> identify the MEP.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) <code>drop l2-bpdu</code> specifies that the switch should drop all data frames, all Layer 3 control traffic, and all Layer 2 BPDU frames except CFM frames for that MEP. If not entered, the switch drops only data frames and Layer 3 control frames.</td>
</tr>
<tr>
<td>19</td>
<td>`ethernet cfm lck start interface interface-id direction {up</td>
<td>down} [drop l2-bpdu]`</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>interface interface-id</code>—Specify the interface to be put in LCK condition.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>direction inward</code>—The LCK is in the direction toward the relay; that is, within the switch.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>direction outward</code>—The LCK is in the direction of the wire.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) <code>drop l2-bpdu</code> specifies that all Layer 2 BPDU frames except CFM frames, all data frames, and all Layer 3 control traffic are dropped for that MEP. If not entered, only data frames and Layer 3 control frames are dropped.</td>
</tr>
<tr>
<td>20</td>
<td><code>show ethernet cfm smep [interface interface-id]</code></td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td>21</td>
<td><code>show ethernet cfm error</code></td>
<td>Display received ETH-LCK frames.</td>
</tr>
<tr>
<td>22</td>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To put a MEP out of LCK condition, enter the `ethernet cfm lck stop mpid local-mpid domain domain-name vlan vlan-id` privileged EXEC command. To put an interface out of LCK condition, enter the `ethernet cfm lck start interface interface-id direction {inward | outward} [drop l2-bpdu]` privileged EXEC command.

This is an example of the output from the `show ethernet cfm smep` command when Ethernet LCK has been enabled:

```
Switch# show ethernet cfm smep
SMEP Settings:
----------------------
Interface: GigabitEthernet1/0/3
LCK-Status: Enabled
LCK Period: 60000 (ms)
Level to transmit LCK: Default
AIS-Status: Enabled
AIS Period: 60000 (ms)
Level to transmit AIS: Default
Defect Condition: AIS
```
Using Multicast Ethernet Loopback

You can use the `ping` privileged EXEC command to verify bidirectional connectivity of a MEP, as in this example:

```
Switch# ping ethernet multicast domain CD vlan 10
Type escape sequence to abort.
Sending 5 Ethernet CFM loopback messages to 0180.c200.0037, timeout is 5 seconds:
Reply to Multicast request via interface FastEthernet1/0/3, from 001a.a17e.f880, 8 ms
Total Loopback Responses received: 1
```

Managing and Displaying Ethernet CFM Information

You can use the privileged EXEC commands in these tables to clear Ethernet CFM information.

### Table 1 Clearing CFM Information

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ethernet cfm ais domain</td>
<td>Clear MEPs with matching domain and VLAN ID out of AIS defect condition.</td>
</tr>
<tr>
<td>domain-name</td>
<td></td>
</tr>
<tr>
<td>mpid id vlan vlan-id</td>
<td></td>
</tr>
<tr>
<td>clear ethernet cfm link-status</td>
<td>Clear a SMEP out of AIS defect condition.</td>
</tr>
<tr>
<td>interface-id</td>
<td></td>
</tr>
<tr>
<td>clear ethernet cfm error</td>
<td>Clear all CFM error conditions, including AIS.</td>
</tr>
</tbody>
</table>

You can use the privileged EXEC commands in Table 43-1 to display Ethernet CFM information.

### Table 43-2 Displaying CFM Information

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ethernet cfm domain [brief]</td>
<td>Displays CFM domain information or brief domain information.</td>
</tr>
<tr>
<td>show ethernet cfm errors [configuration</td>
<td>Displays CFM continuity check error conditions logged on a device since</td>
</tr>
<tr>
<td>domain-id]</td>
<td>it was last reset or the log was last cleared. When CFM crosscheck is</td>
</tr>
<tr>
<td></td>
<td>enabled, displays the results of the CFM crosscheck operation.</td>
</tr>
<tr>
<td>show ethernet cfm maintenance-points local</td>
<td>Displays maintenance points configured on a device.</td>
</tr>
<tr>
<td>[detail</td>
<td>domain</td>
</tr>
<tr>
<td>show ethernet cfm maintenance-points remote</td>
<td>Displays information about a remote maintenance point domains or levels or</td>
</tr>
<tr>
<td>[crosscheck</td>
<td>detail</td>
</tr>
<tr>
<td>show ethernet cfm mpdb</td>
<td>Displays information about entries in the MIP continuity-check database.</td>
</tr>
<tr>
<td>show ethernet cfm smep [interface</td>
<td>Displays Ethernet CFM SMEP information.</td>
</tr>
<tr>
<td>interface-id]</td>
<td></td>
</tr>
<tr>
<td>show ethernet cfm traceroute-cache</td>
<td>Displays the contents of the traceroute cache.</td>
</tr>
<tr>
<td>show platform cfm</td>
<td>Displays platform-independent CFM information.</td>
</tr>
</tbody>
</table>

This is an example of output from the `show ethernet cfm domain brief` command:

```
Switch# show ethernet cfm domain brief
Domain Name                            Index Level Services Archive(min)
level5                                 1   5       1     100
```
This is an example of output from the **show ethernet cfm errors** command:

```
Switch# show ethernet cfm errors
--------------------------------------------------------------------------------
MPID Domain Id  Mac Address     Type   Id   Lvl     Reason     Age
MAName                  Reason                 Age
--------------------------------------------------------------------------------
6307 level3  0021.d7ee.fe80  Vlan    7    3  Receive RDI            5s
vlan7                                                                
```

This is an example of output from the **show ethernet cfm maintenance-points local detail** command:

```
Switch# show ethernet cfm maintenance-points local detail
Local MEPs:                       
----------
MPID: 7307
DomainName: level3
Level: 3
Direction: Up
Vlan: 7
Interface: Gi0/3
CC-Status: Enabled
CC Loss Threshold: 3
MAC: 0021.d7ef.0700
LCK-Status: Enabled
LCK Period: 60000(ms)
LCK Expiry Threshold: 3.5
Level to transmit LCK: Default
Defect Condition: No Defect
presentRDI: FALSE
AIS-Status: Enabled
AIS Period: 60000(ms)
AIS Expiry Threshold: 3.5
Level to transmit AIS: Default
Suppress Alarm configuration: Enabled
Suppressing Alarms: No

MIP Settings:                     
-------------
Local MIPs:                       
* = MIP Manually Configured
--------------------------------------------------------------------------------
Level Port  MacAddress     SrvcInst Type   Id
--------------------------------------------------------------------------------
*5    Gi0/3  0021.d7ef.0700 N/A  Vlan  2,7
```

This is an example of output from the **show ethernet cfm traceroute** command:

```
Switch# show ethernet cfm traceroute
Current Cache-size: 0 Hops
Max Cache-size: 100 Hops
Hold-time: 100 Minutes

You can use the privileged EXEC commands in Table 43-3 to display IP SLAs Ethernet CFM information.
```
Understanding the Ethernet OAM Protocol

The Ethernet OAM protocol for installing, monitoring, and troubleshooting Metro Ethernet networks and Ethernet WANs relies on an optional sublayer in the data link layer of the OSI model. Normal link operation does not require Ethernet OAM. You can implement Ethernet OAM on any full-duplex point-to-point or emulated point-to-point Ethernet link for a network or part of a network (specified interfaces).

OAM frames, called OAM protocol data units (OAM PDUs) use the slow protocol destination MAC address 0180.c200.0002. They are intercepted by the MAC sublayer and cannot propagate beyond a single hop within an Ethernet network. Ethernet OAM is a relatively slow protocol, with a maximum transmission rate of 10 frames per second, resulting in minor impact to normal operations. However, when you enable link monitoring, because the CPU must poll error counters frequently, the number of required CPU cycles is proportional to the number of interfaces that must be polled.

Ethernet OAM has two major components:

- The OAM client establishes and manages Ethernet OAM on a link and enables and configures the OAM sublayer. During the OAM discovery phase, the OAM client monitors OAM PDUs received from the remote peer and enables OAM functionality. After the discovery phase, it manages the rules of response to OAM PDUs and the OAM remote loopback mode.

- The OAM sublayer presents two standard IEEE 802.3 MAC service interfaces facing the superior and inferior MAC sublayers. It provides a dedicated interface for the OAM client to pass OAM control information and PDUs to and from the client. It includes these components:
  - The control block provides the interface between the OAM client and other OAM sublayer internal blocks.
  - The multiplexer manages frames from the MAC client, the control block, and the parser and passes OAM PDUs from the control block and loopback frames from the parser to the subordinate layer.
  - The parser classifies frames as OAM PDUs, MAC client frames, or loopback frames and sends them to the appropriate entity: OAM PDUs to the control block, MAC client frames to the superior sublayer, and loopback frames to the multiplexer.

---

**Table 43-3 Displaying IP SLAs CFM Information**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip sla configuration [entry-number]</code></td>
<td>Displays configuration values including all defaults for all IP SLAs operations or a specific operation.</td>
</tr>
<tr>
<td><code>show ip sla ethernet-monitor configuration [entry-number]</code></td>
<td>Displays the configuration of the IP SLAs automatic Ethernet operation.</td>
</tr>
<tr>
<td>`show ip sla statistics [entry-number</td>
<td>aggregated</td>
</tr>
</tbody>
</table>
OAM Features

These OAM features are defined by IEEE 802.3ah:

- Discovery identifies devices in the network and their OAM capabilities. It uses periodic OAM PDUs to advertise OAM mode, configuration, and capabilities; PDU configuration; and platform identity. An optional phase allows the local station to accept or reject the configuration of the peer OAM entity.

- Link monitoring detects and indicates link faults under a variety of conditions and uses the event notification OAM PDU to notify the remote OAM device when it detects problems on the link. Error events include when the number of symbol errors, the number of frame errors, the number of frame errors within a specified number of frames, or the number of error seconds within a specified period exceed a configured threshold.

- Remote failure indication conveys a slowly deteriorating quality of an OAM entity to its peers by communicating these conditions: Link Fault means a loss of signal, Dying Gasp means an unrecoverable condition, and Critical Event means an unspecified vendor-specific critical event. The switch can receive and process but not generate Link Fault or Critical Event OAM PDUs. It can generate Dying Gasp OAM PDUs to show when Ethernet OAM is disabled, the interface is shut down, the interface enters the error-disabled state, or the switch is reloading. It can respond to, but not generate, Dying Gasp PDUs based on loss of power.

- Remote loopback mode to ensure link quality with a remote peer during installation or troubleshooting. In this mode, when the switch receives a frame that is not an OAM PDU or a pause frame, it sends it back on the same port. The link appears to the user to be in the up state. You can use the returned loopback acknowledgement to test delay, jitter, and throughput.

OAM Messages

Ethernet OAM messages or PDUs are standard length, untagged Ethernet frames between 64 and 1518 bytes. They do not go beyond a single hop and have a maximum transmission rate of 10 OAM PDUs per second. Message types are information, event notification, loopback control, or vendor-specific OAM PDUs.

Setting Up and Configuring Ethernet OAM

This section includes this information:

- Default Ethernet OAM Configuration, page 43-34
- Ethernet OAM Configuration Guidelines, page 43-34
- Enabling Ethernet OAM on an Interface, page 43-34
- Enabling Ethernet OAM Remote Loopback, page 43-35
- Configuring Ethernet OAM Link Monitoring, page 43-36
- Configuring Ethernet OAM Remote Failure Indications, page 43-39
- Configuring Ethernet OAM Templates, page 43-39
Chapter 43      Configuring Ethernet OAM, CFM, and E-LMI

Default Ethernet OAM Configuration

Ethernet OAM is disabled on all interfaces.
When Ethernet OAM is enabled on an interface, link monitoring is automatically turned on.
Remote loopback is disabled.
No Ethernet OAM templates are configured.

Ethernet OAM Configuration Guidelines

Follow these guidelines when configuring Ethernet OAM:

- The switch does not support monitoring of egress frames sent with cyclic redundancy code (CRC) errors. The `ethernet oam link-monitor transmit crc` interface-configuration or template-configuration commands are visible but are not supported on the switch. The commands are accepted, but are not applied to an interface.
- For a remote failure indication, the switch does not generate Link Fault or Critical Event OAM PDUs. However, if these PDUs are received from a link partner, they are processed. The switch supports generating and receiving Dying Gasp OAM PDUs when Ethernet OAM is disabled, the interface is shut down, the interface enters the error-disabled state, or the switch is reloading. It can respond to, but not generate, Dying Gasp PDUs based on loss of power.
- The switch does not support Ethernet OAM on ports that belong to an EtherChannel.

Enabling Ethernet OAM on an Interface

Beginning in privileged EXEC mode, follow these steps to enable Ethernet OAM on an interface:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><code>interface interface-id</code></td>
<td>Define an interface to configure as an EOM interface, and enter interface configuration mode.</td>
</tr>
<tr>
<td><code>ethernet oam</code></td>
<td>Enable Ethernet OAM on the interface.</td>
</tr>
</tbody>
</table>
Setting Up and Configuring Ethernet OAM

Enter the `no ethernet oam` interface configuration command to disable Ethernet OAM on the interface.

### Enabling Ethernet OAM Remote Loopback

You must enable Ethernet OAM remote loopback on an interface for the local OAM client to initiate OAM remote loopback operations. Changing this setting causes the local OAM client to exchange configuration information with its remote peer. Remote loopback is disabled by default.

Remote loopback has these limitations:
- Internet Group Management Protocol (IGMP) packets are not looped back.
- You cannot configure Ethernet OAM remote loopback on ISL ports or ports that belong to an EtherChannel.
- If dynamic ARP inspection is enabled, ARP or reverse ARP packets are not looped or dropped.

Beginning in privileged EXEC mode, follow these steps to enable Ethernet OAM remote loopback on an interface:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><code>interface interface-id</code></td>
<td>Define an interface to configure as an EOM interface, and enter interface configuration mode.</td>
</tr>
</tbody>
</table>
Configuring Ethernet OAM Link Monitoring

You can configure high and low thresholds for link-monitoring features. If no high threshold is configured, the default is none — no high threshold is set. If you do not set a low threshold, it defaults to a value lower than the high threshold.

Beginning in privileged EXEC mode, follow these steps to configure Ethernet OAM link monitoring on an interface:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>ethernet oam link-monitor supported</td>
</tr>
</tbody>
</table>
### Step 4

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ethernet oam link-monitor symbol-period</code></td>
<td>(Optional) Configure high and low thresholds for an error-symbol period that trigger an error-symbol period link event.</td>
</tr>
<tr>
<td>`{ threshold high { high symbols</td>
<td>none }</td>
</tr>
<tr>
<td></td>
<td>- Enter <code>threshold high none</code> to disable the high threshold if it was set. This is the default.</td>
</tr>
<tr>
<td></td>
<td>- Enter <code>threshold low low-symbols</code> to set a low threshold in number of symbols. The range is 0 to 65535. It must be lower than the high threshold.</td>
</tr>
<tr>
<td></td>
<td>- Enter <code>window symbols</code> to set the window size (in number of symbols) of the polling period. The range is 1 to 65535 symbols.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Repeat this step to configure both high and low thresholds.</td>
</tr>
</tbody>
</table>

### Step 5

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ethernet oam link-monitor frame</code></td>
<td>(Optional) Configure high and low thresholds for error frames that trigger an error-frame link event.</td>
</tr>
<tr>
<td>`{ threshold high { high-frames</td>
<td>none }</td>
</tr>
<tr>
<td></td>
<td>- Enter <code>threshold high none</code> to disable the high threshold if it was set. This is the default.</td>
</tr>
<tr>
<td></td>
<td>- Enter <code>threshold low low-frames</code> to set a low threshold in number of frames. The range is 0 to 65535. The default is 1.</td>
</tr>
<tr>
<td></td>
<td>- Enter <code>window milliseconds</code> to set the a window and period of time during which error frames are counted. The range is 10 to 600 and represents the number of milliseconds in multiples of 100. The default is 100.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Repeat this step to configure both high and low thresholds.</td>
</tr>
</tbody>
</table>

### Step 6

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ethernet oam link-monitor frame-period</code></td>
<td>(Optional) Configure high and low thresholds for the error-frame period that triggers an error-frame-period link event.</td>
</tr>
<tr>
<td>`{ threshold high { high-frames</td>
<td>none }</td>
</tr>
<tr>
<td></td>
<td>- Enter <code>threshold high none</code> to disable the high threshold if it was set. This is the default.</td>
</tr>
<tr>
<td></td>
<td>- Enter <code>threshold low low-frames</code> to set a low threshold in number of frames. The range is 0 to 65535. The default is 1.</td>
</tr>
<tr>
<td></td>
<td>- Enter <code>window frames</code> to set the a polling window size in number of frames. The range is 1 to 65535; each value is a multiple of 10000 frames. The default is 1000.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Repeat this step to configure both high and low thresholds.</td>
</tr>
</tbody>
</table>
### Step 7

**Command**

```
ethernet oam link-monitor frame-secs
    {threshold [high [high-frames | none] | low [low-frames]] | window milliseconds}
```

**Purpose**

(Optional) Configure high and low thresholds for the frame-secs error that triggers an error-frame-secs link event.

- Enter `threshold high high-frames` to set a high error frame-secs threshold in number of seconds. The range is 1 to 900. The default is none.
- Enter `threshold high none` to disable the high threshold if it was set. This is the default.
- Enter `threshold low low-frames` to set a low threshold in number of frames. The range is 1 to 900. The default is 1.
- Enter `window frames` to set the a polling window size in number of milliseconds. The range is 100 to 9000; each value is a multiple of 100 milliseconds. The default is 1000.

**Note**

Repeat this step to configure both high and low thresholds.

### Step 8

**Command**

```
ethernet oam link-monitor receive-crc
    {threshold [high [high-frames | none] | low [low-frames]] | window milliseconds}
```

**Purpose**

(Optional) Configure thresholds for monitoring ingress frames received with cyclic redundancy code (CRC) errors for a period of time.

- Enter `threshold high high-frames` to set a high threshold for the number of frames received with CRC errors. The range is 1 to 65535 frames.
- Enter `threshold high none` to disable the high threshold.
- Enter `threshold low low-frames` to set a low threshold in number of frames. The range is 0 to 65535. The default is 1.
- Enter `window milliseconds` to set the a window and period of time during which frames with CRC errors are counted. The range is 10 to 1800 and represents the number of milliseconds in multiples of 100. The default is 100.

**Note**

Repeat this step to configure both high and low thresholds.

### Step 9

```
[no] ethernet link-monitor on
```

(Optional) Start or stop (when the no keyword is entered) link-monitoring operations on the interface. Link monitoring operations start automatically when support is enabled.

### Step 10

```
end
```

Return to privileged EXEC mode.

### Step 11

```
show ethernet oam status [interface interface-id]
```

Verify the configuration.

### Step 12

```
copy running-config startup-config
```

(Optional) Save your entries in the configuration file.

---

The `ethernet oam link-monitor transmit-crc` command is visible on the switch and you are allowed to enter it, but it is not supported. Enter the `no` form of the commands to disable the configuration. Use the `no` form of each command to disable the threshold setting.
Chapter 43 Configuring Ethernet OAM, CFM, and E-LMI

Setting Up and Configuring Ethernet OAM

Configuring Ethernet OAM Remote Failure Indications

You can configure an error-disable action to occur on an interface if one of the high thresholds is exceeded, if the remote link goes down, if the remote device is rebooted, or if the remote device disables Ethernet OAM on the interface.

Beginning in privileged EXEC mode, follow these steps to enable Ethernet OAM remote-failure indication actions on an interface:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Define an interface, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3 ethernet oam remote-failure {critical-event</td>
<td>dying-gasp</td>
</tr>
<tr>
<td></td>
<td>• Select critical-event to shut down the interface when an unspecified critical event has occurred.</td>
</tr>
<tr>
<td></td>
<td>• Select dying-gasp to shut down the interface when Ethernet OAM is disabled or the interface enters the error-disabled state.</td>
</tr>
<tr>
<td></td>
<td>• Select link-fault to shut down the interface when the receiver detects a loss of signal.</td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5 show ethernet oam status [interface interface-id]</td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td>Step 6 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

The switch does not generate Link Fault or Critical Event OAM PDUs. However, if these PDUs are received from a link partner, they are processed. The switch supports sending and receiving Dying Gasp OAM PDUs when Ethernet OAM is disabled, the interface is shut down, the interface enters the error-disabled state, or the switch is reloading. It can respond to, but not generate, Dying Gasp PDUs based on loss of power. Enter the no ethernet remote-failure {critical-event | dying-gasp | link-fault} action command to disable the remote failure indication action.

Configuring Ethernet OAM Templates

You can create a template for configuring a common set of options on multiple Ethernet OAM interfaces. The template can be configured to monitor frame errors, frame-period errors, frame-second errors, received CRS errors, and symbol-period errors and thresholds. You can also set the template to put the interface in error-disabled state if any high thresholds are exceeded. These steps are optional and can be performed in any sequence or repeated to configure different options.
Beginning in privileged EXEC mode, follow these steps to configure an Ethernet OAM template and to associate it with an interface:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>template template-name</td>
</tr>
<tr>
<td></td>
<td>Create a template, and enter template configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>ethernet oam link-monitor receive-crc {threshold [high [high-frames</td>
</tr>
<tr>
<td></td>
<td>(Optional) Configure thresholds for monitoring ingress frames received with cyclic redundancy code (CRC) errors for a period of time.</td>
</tr>
<tr>
<td></td>
<td>• Enter <strong>threshold high</strong> high-frames to set a high threshold for the number of frames received with CRC errors. The range is 1 to 65535 frames.</td>
</tr>
<tr>
<td></td>
<td>• Enter <strong>threshold high</strong> none to disable the high threshold.</td>
</tr>
<tr>
<td></td>
<td>• Enter <strong>threshold low</strong> low-frames to set a low threshold in number of frames. The range is 0 to 65535. The default is 1.</td>
</tr>
<tr>
<td></td>
<td>• Enter <strong>window</strong> milliseconds to set the a window and period of time during which frames with CRC errors are counted. The range is 10 to 1800 and represents the number of milliseconds in multiples of 100. The default is 100.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>ethernet oam link-monitor symbol-period {threshold [high [high-symbols</td>
</tr>
<tr>
<td></td>
<td>(Optional) Configure high and low thresholds for an error-symbol period that triggers an error-symbol period link event.</td>
</tr>
<tr>
<td></td>
<td>• Enter <strong>threshold high</strong> high-symbols to set a high threshold in number of symbols. The range is 1 to 65535.</td>
</tr>
<tr>
<td></td>
<td>• Enter <strong>threshold high</strong> none to disable the high threshold.</td>
</tr>
<tr>
<td></td>
<td>• Enter <strong>threshold low</strong> low-symbols to set a low threshold in number of symbols. The range is 0 to 65535. It must be lower than the high threshold.</td>
</tr>
<tr>
<td></td>
<td>• Enter <strong>window</strong> symbols to set the window size (in number of symbols) of the polling period. The range is 1 to 65535 symbols.</td>
</tr>
</tbody>
</table>
### Step 5

```
ethernet oam link-monitor frame { threshold { high [ high-frames | none ] | low [ low-frames ] } } window milliseconds
```

(Optional) Configure high and low thresholds for error frames that trigger an error-frame link event.

- Enter `threshold high high-frames` to set a high threshold in number of frames. The range is 1 to 65535. You must enter a high threshold.
- Enter `threshold high none` to disable the high threshold.
- Enter `threshold low low-frames` to set a low threshold in number of frames. The range is 0 to 65535. The default is 1.
- Enter `window milliseconds` to set the a window and period of time during which error frames are counted. The range is 10 to 600 and represents the number of milliseconds in a multiple of 100. The default is 100.

### Step 6

```
ethernet oam link-monitor frame-period { threshold { high [ high-frames | none ] | low [ low-frames ] } } window frames
```

(Optional) Configure high and low thresholds for the error-frame period that triggers an error-frame-period link event.

- Enter `threshold high high-frames` to set a high threshold in number of frames. The range is 1 to 65535. You must enter a high threshold.
- Enter `threshold high none` to disable the high threshold.
- Enter `threshold low low-frames` to set a low threshold in number of frames. The range is 0 to 65535. The default is 1.
- Enter `window frames` to set the a polling window size in number of frames. The range is 1 to 65535; each value is a multiple of 10000 frames. The default is 1000.

### Step 7

```
ethernet oam link-monitor frame-seconds { threshold { high [ high-seconds | none ] | low [ low-seconds ] } } window milliseconds
```

(Optional) Configure frame-seconds high and low thresholds for triggering an error-frame-seconds link event.

- Enter `threshold high high-seconds` to set a high threshold in number of seconds. The range is 1 to 900. You must enter a high threshold.
- Enter `threshold high none` to disable the high threshold.
- Enter `threshold low low-frames` to set a low threshold in number of frames. The range is 1 to 900. The default is 1.
- Enter `window frames` to set the a polling window size in number of frames. The range is 100 to 9000; each value is a multiple of 100 milliseconds. The default is 1000.
Displaying Ethernet OAM Protocol Information

You can use the privileged EXEC commands in Table 43-4 to display Ethernet OAM protocol information.

### Table 43-4  Displaying Ethernet OAM Protocol Information

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ethernet oam discovery [interface interface-id]</td>
<td>Displays discovery information for all Ethernet OAM interfaces or the specified interface.</td>
</tr>
<tr>
<td>show ethernet oam statistics [interface interface-id]</td>
<td>Displays detailed information about Ethernet OAM packets.</td>
</tr>
<tr>
<td>show ethernet oam status [interface interface-id]</td>
<td>Displays Ethernet OAM configuration for all interfaces or the specified interface.</td>
</tr>
<tr>
<td>show ethernet oam summary</td>
<td>Displays active Ethernet OAM sessions on the switch.</td>
</tr>
</tbody>
</table>

Understanding E-LMI

Ethernet Local Management Interface (E-LMI) is a protocol between the customer-edge (CE) device and the provider-edge (PE) device. It runs only on the PE-to-CE UNI link and notifies the CE device of connectivity status and configuration parameters of Ethernet services available on the CE port. E-LMI interoperates with an OAM protocol, such as CFM, that runs within the provider network to collect OAM status. CFM runs at the provider maintenance level (UPE to UPE with inward-facing MEPs at the UNI). E-LMI relies on the OAM Ethernet Infrastructure to interwork with CFM for end-to-end status of Ethernet virtual connections (EVCs) across CFM domains.
OAM manager, which streamlines interaction between any two OAM protocols, handles the interaction between CFM and E-LMI. This interaction is unidirectional, running only from OAM manager to E-LMI on the UPE side of the switch. Information is exchanged either as a result of a request from E-LMI or triggered by OAM when it received notification of a change from the OAM protocol. This type of information is relayed:

- EVC name and availability status
- Remote UNI name and status
- Remote UNI counts

You can configure Ethernet virtual connections (EVCs), service VLANs, UNI ids (for each CE-to-PE link), and UNI count and attributes. You need to configure CFM to notify the OAM manager of any change to the number of active UNIs and or the remote UNI ID for a given S-VLAN domain.

You can configure the switch as either the customer-edge device or the provider-edge device.

### E-LMI Interaction with OAM Manager

No interactions are required between E-LMI and OAM manager on the CE side. On the UPE side, OAM manager defines an abstraction layer that relays data collected from OAM protocols (in this case CFM) running within the metro network to the E-LMI switch. The information flow is unidirectional (from OAM manager to the E-LMI) but is triggered in one of two ways:

- Synchronous data flow triggered by a request from the E-LMI
- Asynchronous data flow triggered by OAM manager when it receives notification from CFM that the number of remote UNIs has changed

This data includes:

- EVC name and availability status (active, not active, partially active, or not defined)
- Remote UNI name and status (up, disconnected, administratively down, excessive FCS failures, or not reachable)
- Remote UNI counts (the total number of expected UNIs and the actual number of active UNIs)

The asynchronous update is triggered only when the number of active UNIs has changed.

### CFM Interaction with OAM Manager

When there is a change in the number of active UNIs or remote UNI ID for a given S-VLAN or domain, CFM asynchronously notifies the OAM manager. A change in the number of UNIs might (or might not) cause a change in EVC status. OAM manager calculates EVC status given the number of active UNIs and the total number of associated UNIs.

---

**Note**

If crosscheck is disabled, no SNMP traps are sent when there is a change in the number of UNIs.
Configuring E-LMI

For E-LMI to work with CFM, you configure Ethernet virtual connections (EVCs), Ethernet service instances (EFPs), and E-LMI customer VLAN mapping. Most of the configuration occurs on the PE switch on the interfaces connected to the CE device. On the CE switch, you only need to enable E-LMI on the connecting interface. Note that you must configure some OAM parameters, for example, EVC definitions, on PE devices on both sides of a metro network.

This section includes this information:

- Default E-LMI Configuration, page 43-44
- E-LMI and OAM Manager Configuration Guidelines, page 43-44
- Configuring the OAM Manager, page 43-45
- Enabling E-LMI, page 43-47
- Ethernet OAM Manager Configuration Example, page 43-48

Default E-LMI Configuration

Ethernet LMI is globally disabled by default. When enabled, the switch is in provider-edge (PE) mode by default.

When you globally enable E-LMI by entering the `ethernet lmi global` global configuration command, it is automatically enabled on all interfaces. You can also enable or disable E-LMI per interface to override the global configuration. The E-LMI command that is given last is the command that has precedence.

There are no EVCs, EFP service instances, or UNIs defined.

UNI bundling service is bundling with multiplexing.

E-LMI and OAM Manager Configuration Guidelines

OAM manager is an infrastructural element and requires two interworking OAM protocols, in this case CFM and E-LMI. For OAM to operate, the PE side of the connection must be running CFM and E-LMI.

- E-LMI is not supported on routed ports, EtherChannel port channels or ports that belong to an EtherChannel, private VLAN ports, IEEE 802.1Q tunnel ports, or EoMPLS ports.
- You cannot configure E-LMI on VLAN interfaces.
- When you enable E-LMI globally or on an interface, the switch is in PE mode by default. You must enter the `ethernet lmi ce` global configuration command to enable the switch or interface in customer-edge mode.
- When the switch is configured as a CE device, the `service instance` and `ethernet uni` interface commands are visible but not supported.
Configuring the OAM Manager

Beginning in privileged EXEC mode, follow these steps to configure OAM manager on a PE switch:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>ethernet cfm domain domain-name level level-id</td>
<td>Define a CFM domain, set the domain level, and enter ethernet-cfm configuration mode for the domain. The maintenance level number range is 0 to 7.</td>
</tr>
</tbody>
</table>
| 3    | service csi-id vlan vlan-id | Define a universally unique customer service instance (CSI) and VLAN ID within the maintenance domain.  
- csi-id—a string of no more than 100 characters that identifies the CSI.  
- vlan-id—VLAN range is from 1 to 4095. You cannot use the same VLAN ID for more than one domain at the same level. |
| 4    | exit | Return to global configuration mode. |
| 5    | ethernet evc evc-id | Define an Ethernet virtual connection (evc), and enter evc configuration mode. The identifier can be up to 100 characters in length. |
| 6    | oam protocol cfm svlan vlan-id domain domain-name | Configure the EVC OAM protocol as CFM, and identify the service provider VLAN-ID (S-VLAN-ID) for the CFM domain maintenance level as configured in Steps 2 and 3.  
**Note** If the CFM domain does not exist, the command is rejected, and an error message appears. |
| 7    | uni count value | (Optional) Set the UNI count for the EVC. The range is 2 to 1024; the default is 2.  
If the command is not entered, the service defaults to a point-to-point service. If you enter a value of 2, you have the option to select point-to-multipoint service. If you configure a value of 3 or greater, the service is point-to-multipoint.  
**Note** You should know the correct number of maintenance end points in the domain. If you enter a value greater than the actual number of end points, the UNI status will show as partially active even if all end points are up; if you enter a uni count less than the actual number of end points, status might show as active, even if all end points are not up. |
| 8    | exit | Return to global configuration mode. |
| 9    | Repeat Steps 2 to 5 for other CFM domains that you want OAM manager to monitor. |
| 10   | interface interface-id | Specify a physical interface connected to the CE device, and enter interface configuration mode. |
### Configuring E-LMI

| Step 11 | **service instance efp-identifier ethernet [evc-id]** | Configure an Ethernet service instance (EFP) on the interface, and enter ethernet service configuration mode.  
  - The EFP identifier is a per-interface service identifier that does not map to a VLAN. The EFP identifier range is 1 to 4967295.  
  - (Optional) Enter an `evc-id` to attach an EVC to the EFP. |
| --- | --- | --- |
| Step 12 | **ethernet lmi ce-vlan map [vlan-id | any | default | untagged]** | Configure an E-LMI customer VLAN-to-EVC map for a particular UNI. The keywords have these meanings:  
  - For `vlan vlan-id`, enter the customer VLAN ID or IDs to map to as single VLAN-ID (1 to 4094), a range of VLAN-IDs separated by a hyphen, or a series of VLAN IDs separated by commas.  
  - Enter `any` to map all VLANs (untagged or 1 to 4094).  
  - Enter `default` to map the default EFP. You can use `default` keyword only if you have already mapped the service instance to a VLAN or group of VLANs.  
  - Enter `untagged` to map untagged VLANs. |
| Step 13 | **exit** | Return to interface configuration mode. |
| Step 14 | **ethernet uni id name** | Configure an Ethernet UNI ID. The name should be unique for all the UNIs that are part of a given customer service instance and can be up to 64 characters in length. When a UNI id is configured on a port, that ID is used as the default name for all MEPs configured on the port, unless a name is explicitly configured for a given MEP.  
**Note** This command is required on all ports that are directly connected to CE devices. If the specified ID is not unique on the device, an error message appears. |
| Step 15 | **ethernet uni {bundle [all-to-one] | multiplex}** | (Optional) Set UNI bundling attributes:  
  - If you enter `bundle` `<cr>`, the UNI supports bundling without multiplexing (only one EVC with one or multiple VLANs be mapped to it).  
  - If you enter `bundle all-to-one`, the UNI supports a single EVC and all VLANs are mapped to that EVC.  
  - If you enter `multiplex`, the UNI supports multiplexing without bundling (one or more EVCs with a single VLAN mapped to each EVC).  
If you do not configure bundling attributes, the default is bundling with multiplexing (one or more EVCs with one or more VLANs mapped to each EVC). |
| Step 16 | **end** | Return to privileged EXEC mode. |
| Step 17 | **show ethernet service evc {detail | id evc-id | interface interface-id}** | Verify the configuration. |
| Step 18 | **copy running-config startup-config** | (Optional) Save your entries in the configuration file. |
Use the `no` forms of the commands to delete an EVC, EFP, or UNI ID, or to return to default configurations.

**Note**
If you configure, change, or remove a UNI service type, EVC, EFP, or CE-VLAN configuration, all configurations are checked to make sure that the configurations match (UNI service type with EVC or EFP and CE-VLAN configuration). The configuration is rejected if the configurations do not match.

### Enabling E-LMI

You can enable E-LMI globally or on an interface and you can configure the switch as a PE or a CE device. Beginning in privileged EXEC mode, follow these steps to enable for E-LMI on the switch or on an interface. Note that the order of the global and interface commands determines the configuration. The command that is entered last has precedence.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>ethernet lmi global</td>
<td>Globally enable E-LMI on all interfaces. By default, the switch is a PE device.</td>
</tr>
<tr>
<td>Step 3</td>
<td>ethernet lmi ce</td>
<td>(Optional) Configure the switch as an E-LMI CE device.</td>
</tr>
<tr>
<td>Step 4</td>
<td>interface interface-id</td>
<td>Define an interface to configure as an E-LMI interface, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 5</td>
<td>ethernet lmi interface</td>
<td>Configure Ethernet LMI on the interface. If E-LMI is enabled globally, it is enabled on all interfaces unless you disable it on specific interfaces. If E-LMI is disabled globally, you can use this command to enable it on specified interfaces.</td>
</tr>
</tbody>
</table>
Configuring E-LMI

Use the `no ethernet lmi` global configuration command to globally disable E-LMI. Use the `no` form of the `ethernet lmi` interface configuration command with keywords to disable E-LMI on the interface or to return the timers to the default settings.

Use the `show ethernet lmi` commands to display information that was sent to the CE from the status request poll. Use the `show ethernet service` commands to show current status on the device.

**Ethernet OAM Manager Configuration Example**

This is a simple example of configuring CFM and E-LMI with OAM manager on a PE device and on a CE device. You can configure the switch as either the PE device or the CE device.

**Provider-Edge Device Configuration**

This example shows a sample configuration of OAM manager, CFM, and E-LMI on the PE device:

```
Switch# config t
Switch(config)# ethernet cfm domain Top level 7
Switch(config)# ethernet cfm domain Provider level 4
Switch(config-ether-cfm)# service customer_1 vlan 101
Switch(config-ether-cfm)# mep crosscheck mpid 404 vlan 101
Switch(config-ether-cfm)# exit
Switch(config)# ethernet cfm domain Operator_level 2
Switch(config-ether-cfm)# service operator_1 vlan 101
```
Switch(config-ether-cfm)# exit
Switch(config)# ethernet cfm enable
Switch(config)# ethernet evc test1
Switch(config-evc)# oam protocol cfm svlan 101 domain Provider
Switch(config-evc)# exit
Switch(config)# ethernet evc 101
Switch(config-evc)# uni count 3
Switch(config-evc)# oam protocol cfm svlan 101 domain Operator
Switch(config-evc)# exit
Switch(config)# ethernet evc 101
Switch(config-evc)# uni count 3
Switch(config-evc)# oam protocol cfm svlan 101 domain Operator
Switch(config-evc)# exit
Switch(config)# ethernet lmi global
Switch(config)# interface gigabitethernet 1/0/2
Switch(config-if)# ethernet cfm mip level 7
Switch(config-if)# ethernet cfm mep level & mpid 200 vlan 200
Switch(config-if)# service instance 101 ethernet test1
Switch(config-if-srv)# ethernet lmi ce-vlan map 101
Switch(config-if-srv)# exit
Switch(config-if)# exit
Switch(config)# ethernet cfm cc enable level 2-4 vlan 101
Switch(config)# exit

Customer-Edge Device Configuration

This example shows the commands necessary to configure E-LMI on the CE device. Beginning with Cisco IOS Release 12.2(37)SE, the switch can be configured as the CE device.

This example enables E-LMI globally, but you can also enable it only on a specific interface. However, if you do not enter the ethernet lmi ce global configuration command, the interface will be in PE mode by default.

Switch# config t
Switch(config)# ethernet lmi global
Switch(config)# ethernet lmi ce
Switch(config)# exit

Note

For E-LMI to work, any VLANs used on the PE device must also be created on the CE device. Create a VLAN by entering the `vlan vlan-id` global configuration command on the CE device, where the `vlan-ids` match those on the PE device and configure these VLANs as allowed VLANs by entering the `switchport trunk allowed vlan` command on the PE device. Allowed VLANs can receive and send traffic on the interface in tagged format when in trunking mode.

Displaying E-LMI and OAM Manager Information

You can use the privileged EXEC commands in Table 43-5 to display E-LMI or OAM manager information.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ethernet lmi evc [detail evc-id [interface interface-id]</td>
<td>map interface type number]</td>
</tr>
<tr>
<td>show ethernet lmi parameters interface interface-id</td>
<td>Displays Ethernet LMI interface parameters sent to the CE from the status request poll.</td>
</tr>
</tbody>
</table>
Ethernet CFM and Ethernet OAM Interaction

Beginning with Cisco IOS Release 12.2(40)SE, you can also configure the OAM Manager infrastructure for interaction between CFM and Ethernet OAM. When the Ethernet OAM Protocol is running on an interface that has CFM MEPs configured, Ethernet OAM informs CFM of the state of the interface. Interaction is unidirectional from the Ethernet OAM to the CFM Protocol, and the only information exchanged is the user network interface port status.

The Ethernet OAM Protocol notifies CFM when these conditions occur:

- Error thresholds are crossed at the local interface.
  
  CFM responds to the notification by sending a port status of *Local_Excessive_Errors* in the Port StatusType Length Value (TLV).

- Ethernet OAM receives an OAMPDU from the remote side showing that an error threshold is exceeded on the remote endpoint.

  CFM responds to the notification by sending a port status of *Remote_Excessive_Errors* in the Port Status TLV.

- The local port is set into loopback mode.

  CFM responds by sending a port status of Test in the Port Status TLV.

- The remote port is set into loopback mode.

  CFM responds by sending a port status of Test in the Port Status TLV.

This section includes this information:

- Configuring Ethernet OAM Interaction with CFM, page 43-51
- Ethernet OAM and CFM Configuration Example, page 43-52

For more information about CFM and interaction with Ethernet OAM, see the *Cisco IOS Carrier Ethernet Configuration Guide*:


### Table 43-5  Displaying E-LMI and OAM Manager Information (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ethernet lmi statistics interface <em>interface-id</em></td>
<td>Displays Ethernet LMI interface statistics sent to the CE from the status request poll.</td>
</tr>
<tr>
<td>show ethernet lmi uni map interface [interface-id]</td>
<td>Displays information about the E-LMI UNI VLAN map sent to the CE from the status request poll.</td>
</tr>
<tr>
<td>show ethernet service evc {detail</td>
<td>id <em>evc-id</em></td>
</tr>
<tr>
<td>show ethernet service instance {detail</td>
<td>id <em>efp-identifier</em> interface <em>interface-id</em></td>
</tr>
<tr>
<td>show ethernet service interface [interface-id] [detail]</td>
<td>Displays information about OAM manager interfaces.</td>
</tr>
</tbody>
</table>
Configuring Ethernet OAM Interaction with CFM

For Ethernet OAM to function with CFM, you must configure an Ethernet Virtual Circuit (EVC) and the OAM manager, and associate the EVC with CFM. You must use an inward facing MEP for interaction with the OAM manager.

**Note**
If you configure, change, or remove a UNI service type, EVC, Ethernet service instance, or CE-VLAN configuration, all configurations are verified to ensure that the UNI service types match the EVC configuration and that Ethernet service instances are matched with the CE-VLAN configuration. Configurations are rejected if the pairs do not match.

Configuring the OAM Manager

Beginning in privileged EXEC mode, follow these steps to configure the OAM manager on a PE device:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>ethernet cfm domain domain-name level level-id</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>service csi-id vlan vlan-id</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>exit</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>ethernet evc evc-id</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>oam protocol cfm svlan vlan-id domain domain-name</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>exit</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>Repeat Steps 2 through 7 to define other CFM domains that you want OAM manager to monitor.</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>ethernet cfm enable</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>
Enabling Ethernet OAM

Beginning in privileged EXEC mode, follow these steps to enable Ethernet OAM on an interface.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
configure terminal                          | Enter global configuration mode.                                        |
| **Step 2**
interface interface-id                       | Define an interface to configure as an Ethernet OAM interface and enter interface configuration mode. |
| **Step 3**
ethernet oam [max-rate oampdus | min-rate seconds | mode {active | passive} | timeout seconds] | Enable Ethernet OAM on the interface  |
|                                              | (Optional) Enter **max-rate oampdus** to set the maximum rate (per second) to send OAM PDUs. The range is 1 to 10 PDUs per second; the default is 10. |
|                                              | (Optional) Enter **min-rate seconds** to set the minimum rate in seconds. The range is 1 to 10 seconds. |
|                                              | (Optional) Set the OAM client **mode** as **active** or **passive**. The default is **active**. |
|                                              | (Optional) Enter **timeout seconds** to set the time after which a device declares the OAM peer to be nonoperational and resets its state machine. The range is 2 to 30 seconds; the default is 5 seconds. |
| **Step 4**
end                                           | Return to privileged EXEC mode.                                          |
| **Step 5**
copy running-config startup-config             | (Optional) Save your entries in the configuration file.                 |
| **Step 6**
show ethernet cfm maintenance points remote    | (Optional) Display the port states as reported by Ethernet OAM.         |

Ethernet OAM and CFM Configuration Example

These are example configurations of the interworking between Ethernet OAM and CFM in a sample service provider network with a provider-edge switch connected to a customer edge switch at each endpoint. You must configure CFM, E-LMI, and Ethernet OAM between the customer edge and the provider edge switch.

Customer-edge switch 1 (CE1) configuration:
```
Switch# config t
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# switchport trunk allowed vlan 10
Switch(config-if)# switchport mode trunk
Switch(config-if)# ethernet oam remote-loopback supported
Switch(config-if)# ethernet oam
Switch(config-if)# exit
```

Provider-edge switch 1 (PE1) configuration:
```
Switch# config t
Switch(config)# interface fastethernet1/0/20
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# ethernet cfm mip level 7
Switch(config-if)# ethernet cfm mep level 4 mpid 100 vlan 10
Switch(config-if)# ethernet uni id 2004-20
```
Switch(config-if)# ethernet oam remote-loopback supported
Switch(config-if)# ethernet oam
Switch(config-if)# service instance 10 ethernet BLUE
Switch(config-if-srv)# ethernet lmi ce-vlan map 10
Switch(config-if-srv)# exit

Provider-edge switch 2 (PE2) configuration:
Switch# config t
Switch(config)# interface gigabitethernet1/1/20
Switch(config-if)# switchport mode trunk
Switch(config-if)# ethernet cfm mip level 7
Switch(config-if)# ethernet cfm mep level 4 mpid 101 vlan 10
Switch(config-if)# ethernet uni id 2004-20
Switch(config-if)# ethernet oam remote-loopback supported
Switch(config-if)# ethernet oam
Switch(config-if)# service instance 10 ethernet BLUE
Switch(config-if-srv)# ethernet lmi ce-vlan map 10
Switch(config-if-srv)# exit

Customer-edge switch 2 (CE2) configuration:
Switch# config t
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# switchport trunk allowed vlan 10
Switch(config-if)# switchport mode trunk
Switch(config-if)# ethernet oam remote-loopback supported
Switch(config-if)# ethernet oam
Switch(config-if)# exit

These are examples of the output showing provider-edge switch port status of the configuration. Port status shows as **UP** at both switches.

Switch PE1:
Switch# show ethernet cfm maintenance points remote
MPID  Level  Mac Address  Vlan  PortState  InGressPort  Age(sec)  Service ID
101 * 4  0015.633f.6900  10   UP        Gi1/1/1         27       blue

Switch PE2:
Switch# show ethernet cfm maintenance points remote
MPID  Level  Mac Address  Vlan  PortState  InGressPort  Age(sec)  Service ID
100 * 4  0012.00a3.3780  10   UP        Gi1/1/1         8        blue

Total Remote MEPs: 1

This example shows the outputs when you start remote loopback on CE1 (or PE1). The port state on the remote PE switch shows as **Test** and the remote CE switch goes into error-disable mode.

Switch# ethernet oam remote-loopback start interface gigabitEthernet 0/1
This is a intrusive loopback.
Therefore, while you test Ethernet OAM MAC connectivity, you will be unable to pass traffic across that link.
Proceed with Remote Loopback? [confirm]

Switch PE1:
Switch# show ethernet cfm maintenance points remote
MPID  Level  Mac Address  Vlan  PortState  InGressPort  Age(sec)  Service ID
101 * 4  0015.633f.6900  10   UP        Gi1/1/1         27       blue
Switch PE2:

```
Switch# show ethernet cfm maintenance points remote
MPID  Level Mac Address    Vlan PortState InGressPort   Age(sec) Service ID
100 * 4  0012.00a3.3780 10   TEST   Gi1/1/1         8        blue
Total Remote MEPs: 1
```

In addition, if you shut down the CE1 interface that connects to PE1, the remote PE2 port will show a PortState of *Down*. 
Configuring MPLS, MPLS VPN, MPLS OAM, and EoMPLS

This chapter describes how to configure multiprotocol label switching (MPLS) and Ethernet over MPLS (EoMPLS) on the Catalyst 3750 Metro switch. MPLS is a packet-switching technology that integrates link layer (Layer 2) switching with network layer (Layer 3) routing. With MPLS, data is transferred over any combination of Layer 2 technologies, using any Layer 3 protocol, with increased scalability. MPLS supports different routes between a source and destination over a router-based Internet backbone.

- MPLS virtual private networks (VPNs) provides the capability to deploy and administer scalable Layer 3 VPN backbone services to business customers. A VPN is a secure IP-based network that shares resources on one or more physical networks.

- Cisco IOS Release 12.2(37)SE includes support for MPLS Operations, Administration, and Maintenance (OAM) functionality to allow service providers to monitor label switched path (LSP) integrity and to quickly isolate MPLS forwarding problems. Cisco IOS Release 12.2(40)SE adds more functionality, including support for MPLS IP Service Level Agreements (IP SLAs).

- Cisco IOS Release 12.2(46)SE adds support for MPLS traffic engineering fast reroute link protection. This feature provides link protection to label-switched paths (LSPs), enabling LSP traffic that crosses a failed link to be rerouted around the failure.

- EoMPLS is a tunneling mechanism that transports Layer 2 Ethernet frames over an MPLS network. You can connect two Layer 2 networks that are in different locations, without bridges, routers, or switches at the locations. You enable the MPLS backbone to accept Layer 2 traffic by configuring the label-edge routers (LERs) at both ends of the MPLS backbone.

MPLS functionality is supported only on the enhanced-services (ES) ports; EoMPLS is supported on standard ports and on switch virtual interfaces (SVIs).

Note

The switch does not support IPv6 features with any ES port features, such as MPLS. MPLS and EoMPLS are mutually exclusive with IPv6.

For more information about MPLS, see the “Multiprotocol Label Switching” section of the Cisco IOS Multiprotocol Label Switching Configuration Guide for Release 12.2 at this URL:

For complete syntax and usage information for the MPLS commands used in this chapter, see this URL:
This chapter contains these sections:

- Understanding MPLS Services, page 44-2
- Understanding MPLS VPNs, page 44-3
- Configuring MPLS VPNs, page 44-6
- Understanding MPLS Traffic Engineering and Fast Reroute, page 44-13
- Configuring MPLS Traffic Engineering and Fast Reroute, page 44-15
- Understanding MPLS OAM, page 44-21
- Configuring MPLS OAM and IP SLAs MPLS, page 44-25
- Understanding EoMPLS, page 44-40
- Enabling EoMPLS, page 44-43
- Configuring MPLS and EoMPLS QoS, page 44-51
- Monitoring and Maintaining MPLS and EoMPLS, page 44-55

The switch supports hierarchical virtual private LAN service (H-VPLS) architecture to simulate LAN services over the MPLS network. The switch supports H-VPLS using IEEE 802.1Q tunneling or Ethernet over multiprotocol label switching (EoMPLS). For more information, see these software documents:

- For information about EoMPLS, see the “Understanding EoMPLS” section on page 44-40.
- For information about configuring EoMPLS, see the “Enabling EoMPLS” section on page 44-43.
- For information about IEEE 802.1Q tunneling, see the “Configuring IEEE 802.1Q and Layer 2 Protocol Tunneling” chapter.
- For information about configuring H-VPLS on Cisco 7600 routers, see the “Configuring Multiprotocol Label Switching on the Optical Services Modules” section in the OSM Configuration Note, 12.2SX at:

**Understanding MPLS Services**

In conventional Layer 3 forwarding, as a packet travels across the network, each router extracts the packet-forwarding information from the Layer 3 header and uses this information as a key for a routing table lookup to determine the packet's next hop. In most cases, the only relevant field in the header is the destination address field, but in some cases other header fields are also relevant. For this reason, each router through which the packet passes must analyze the packet header.

With MPLS, the Layer 3 header is analyzed only once and then is mapped into a fixed-length, unstructured value called a label. Many different headers can map to the same label, as long as those headers always result in the same choice of next hop. In effect, a label represents a forwarding-equivalence class (FEC)—that is, a set of packets that can be very different but that are indistinguishable to the forwarding function.

The initial choice of label can be based exclusively on the contents of the Layer 3 header, or it can be based on policy, allowing forwarding decisions at subsequent hops to be based on policy. After a label is chosen, a short label header is put at the front of the Layer 3 packet and carried across the network as part of the packet. At subsequent hops through each MPLS router in the network, labels are exchanged,
and the router uses MPLS forwarding-table lookups for the label to make forwarding decisions. It is not necessary to re-analyze the packet header. Because the label is a fixed length and unstructured, the MPLS forwarding-table lookup process is straightforward and fast.

Each label-switching router (LSR) in the network makes an independent, local decision as to which label value is used to represent which forwarding equivalence class. This association is known as a label binding. Each LSR informs its neighbors of the label bindings that it has made. When a labeled packet is sent from LSR A to neighboring LSR B, the label value carried by the packet is the label value that B assigned to represent the packet’s forwarding equivalence class. Thus, the label value changes as the IP packet travels through the network.

Note

Because the Catalyst 3750 Metro switch is used as service-provider edge (PE) device, rather than a service-provider core router, it does not normally operate as an LSR. The switch only performs label switching when it is connected to two different provider core routers over the ES ports to provide a redundant path. In this case, the switch uses quality of service (QoS) policies to classify MPLS packets on egress for label switching.

A label represents a forwarding-equivalence class, but it does not represent a particular path through the network. In general, the path through the network continues to be chosen by the existing Layer 3 routing protocols, such as Open Shortest Path First (OSPF), Enhanced Interior Gateway Protocol (EIGRP), Intermediate-System-to-Intermediate-System (IS-IS), and Border Gateway Protocol (BGP). At each hop when a label is looked up, the choice of the next hop is determined by the dynamic routing algorithm.

**Understanding MPLS VPNs**

Using MPLS virtual private networks (VPNs) provides the capability to deploy and administer scalable Layer 3 VPN backbone services to business customers. A VPN is a secure IP-based network that shares resources on one or more physical networks. A VPN contains geographically dispersed sites that can communicate securely over a shared backbone.

VPN routes are distributed over the MPLS network by using multiprotocol BGP (MP-BGP), which also distributes the labels associated with each VPN route. MPLS VPN depends on VPN routing and forwarding (VRF) support to isolate the routing domains from each other. When routes are learned over an MPLS VPN, the switch learns the new route as a normal VRF route, except that the destination MAC address for the next hop is not the real address, but a specially formed address that contains an identifier that is allocated for the route. When an MPLS-VPN packet is received on a port, the switch looks up the labels in the routing table to determine what to do with the packet.

Each VPN is associated with one or more VPN VRF instances. A VRF includes routing and forwarding tables and rules that define the VPN membership of customer devices attached to the customer-edge (CE) device. A customer site can be a member of multiple VPNs; however, a site can associate with only one VRF. A VRF has these elements:

- An IP routing table
- A Cisco Express Forwarding table
- A set of interfaces that use the forwarding table
- A set of rules and routing protocol parameters to control the information in the routing tables

A customer-site VRF contains all the routes available to the site from the VPNs to which it belongs. VPN routing information is stored in the IP routing table and the Cisco Express Forwarding table for each VRF. A separate set of tables is maintained for each VRF, which prevents information from being
forwarded outside a VPN and prevents packets that are outside a VPN from being forwarded to a router within the VPN. Based on the routing information stored in the VRF IP routing table and the VRF Cisco Express Forwarding table, packets are forwarded to their destinations.

A provider-edge router binds a label to each customer prefix that is learned from a CE device and includes the label in the network reachability information for the prefix that it advertises to other (PE) routers. When a PE router forwards a packet that is received from a CE device across the provider network, it labels the packet with the label learned from the destination PE router. When the destination PE router receives the labeled packet, it examines the label and uses it to direct the packet to the correct CE device.

A customer data-packet carries two levels of labels when traversing the backbone:

- The top label directs the packet to the correct PE router.
- The second label defines how that PE router should forward the packet to the CE device.

**VPN Benefits**

MPLS VPNs allow service providers to deploy scalable VPNs and build the foundation to deliver value-added services, including:

- **Connectionless service**—MPLS VPNs are connectionless, which means that no prior action is required to establish communication between hosts. A connectionless VPN does not require tunnels and encryption for network privacy.

- **Centralized service**—MPLS VPNs are seen as private intranets, which allows delivery of targeted IP services to a group of users represented by a VPN.

- **Scalability**—MPLS-based VPNs use the peer model and Layer 3 connectionless architecture to leverage a highly scalable solution. The peer model requires a customer site to act as a peer to one PE router as opposed to all other customer PE or CE devices that are members of the VPN. The PE routers maintain VPN routes for those VPNs that are members. Routers in the core network do not maintain any VPN routes.

- **Security**—MPLS VPNs offer the same level of security as connection-oriented VPNs. Packets from one VPN do not inadvertently go to another VPN. Security provided at the edge of a provider network ensures that packets received from a customer are placed on the correct VPN; security provided at the backbone ensures that VPN traffic is kept separate.

- **Easy to create**—Because MPLS VPNs are connectionless, no specific point-to-point connection maps or topologies are required, and you can add sites to intranets and extranets to form closed user groups.

- **Flexible addressing**—Customers can continue to use their present address spaces without network address translation (NAT) because the MPLS VPN provides a public and private view of the address. A NAT is required only if two VPNs with overlapping address spaces want to communicate.

- **Straightforward migration**—You can build MPLS VPNs over multiple network architectures. Migration for the end customer is simplified because the CE router is not required to support MPLS, so no customer's intranet modifications are needed.

- **MPLS VPN also provides increased BGP functionality.**

Figure 44-1 shows an example of a VPN with a service-provider backbone network, provider-edge (PE) CLE routers, and customer-edge (CE) devices.
Understanding MPLS VPNs

Each VPN contains customer devices attached to the customer-edge (CE) devices. The customer devices use VPNs to exchange information between devices, and the provider routers (P) are not aware of the VPNs.

Figure 44-2 shows five customer sites communicating within three VPNs. The VPNs can communicate with these sites:

VPN1: Sites 2 and 4
VPN2: Sites 1, 3, and 4
VPN3: Sites 1, 3, and 5

Figure 44-2 Customer Sites with VPNs
Distribution of VPN Routing Information

The distribution of VPN routing information is controlled through the use of VPN route target communities, implemented by BGP extended communities. VPN routing information is distributed in this manner:

- When a VPN route learned from a CE device is added to the BGP process, a list of VPN route target extended community attributes is associated with it. The attribute values are obtained from an export list of route targets associated with the VRF from which the route was learned.
- An import list of route target extended communities is also associated with each VRF. The import list defines route target extended community attributes that a route must have in order for the route to be imported into the VRF. For example, if the import list for a particular VRF includes route target communities A, B, and C, then any VPN route that carries any of those route target extended communities—A, B, or C—is imported into the VRF.

A PE router can learn an IP prefix from a CE device by static configuration, through a BGP session with the CE device, or through the Routing Information Protocol (RIP) exchange with the CE router. The IP prefix is a member of the IPv4 address family. After it learns the IP prefix, the PE router converts it into a VPN-IPv4 prefix by combining it with an 8-byte route distinguisher. The generated prefix is a member of the VPN-IPv4 address family and uniquely identifies the customer address, even if the customer site is using globally nonunique (unregistered private) IP addresses.

BGP distributes reachability information for VPN-IPv4 prefixes for each VPN. BGP communication takes place at two levels: within IP domains, known as autonomous systems (internal BGP or IBGP), and between autonomous systems (external BGP or EIBGP). The PE-to-PE sessions are IBGP sessions, and PE-to-CE sessions are EBGP sessions.

BGP propagates reachability information for VPN-IPv4 prefixes among provider-edge routers by using the BGP multiprotocol extensions, which define support for address families other than IPv4. It does this in a way that ensures that the routes for a given VPN are learned only by other members of that VPN, which enables members of the VPN to communicate with each other.

Configuring MPLS VPNs

This section includes this information about configuring MPLS VPNs on a Catalyst 3750 Metro switch used as a PE router:

- Default MPLS Configuration, page 44-7
- MPLS VPN Configuration Guidelines, page 44-7

These sections describe the required tasks:

- Enabling MPLS, page 44-7
- Defining VPNs, page 44-8
- Configuring BGP Routing Sessions, page 44-9
- Configuring Provider-Edge-to-Provider-Edge Routing Sessions, page 44-10

You must also configure a provider-edge-to-customer-edge routing session. These sections provide example configurations:

- Configuring BGP Provider-Edge-to-Customer-Edge Routing Sessions, page 44-10
- Configuring RIP Provider-Edge-to-Customer-Edge Routing Sessions, page 44-11
- Configuring Static Route Provider-Edge-to-Customer-Edge Routing Sessions, page 44-11
For an example of packet flow in an MPLS VPN, see the “Packet Flow in an MPLS VPN” section on page 44-12.

**Default MPLS Configuration**

By default, label switching of IPv4 packets along normally routed paths is globally enabled. MPLS forwarding of IPv4 packets is disabled by default on interfaces.

If no distribution protocol is explicitly configured by the `mpls label protocol` global configuration command, tag distribution protocol (TDP) is the default label distribution protocol for the switch. Cisco recommends that you configure label distribution protocol (LDP) for MPLS.

If no protocol is explicitly configured for an interface, the default label distribution protocol for the switch is used. By default, the labels of all destinations are advertised to all LDP neighbors.

No VRFs are defined. The default routing table for an interface is the global routing table.

**MPLS VPN Configuration Guidelines**

Follow these guidelines when configuring MPLS VPN:

- MPLS requires that CEF is enabled on the switch. CEF is enabled by default. For more information about CEF, see the “Configuring Cisco Express Forwarding” section on page 36-98.
- The switch must connect to the MPLS network through an ES port. MPLS configuration is supported only on ES ports.
- Do not configure VLAN mapping on an interface configured for MPLS.
- The switch supports a total of 26 VRFs and VPNs.
- VRFs are not compatible with the PBR template. If you configure the PBR template by entering the `sdm prefer routing-pbr` command, any preconfigured VRFs are removed from the configuration. PBR and VRFs cannot function on the same switch.
- MPLS VPN and QoS—you can apply standard QoS functions to MPLS VPN traffic. However, for a hierarchical QoS function, you cannot apply a service policy that would match traffic on a per VRF basis because VRFs are dynamically assigned to an MPLS label. For MPLS VPN traffic, you can apply a service-policy on egress that matches traffic based on DSCP or MPLS.

**Enabling MPLS**

To use MPLS in a network, such as the one shown in Figure 44-1, MPLS must be globally enabled and explicitly configured on the provider-edge routers.

Beginning in privileged EXEC mode, follow these steps to incrementally deploy MPLS through a network, assuming that packets to all destination prefixes should be label-switched:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>ip routing</td>
<td>Enable IP routing on the switch if it is disabled.</td>
</tr>
<tr>
<td>3</td>
<td>ip cef distributed</td>
<td>Enable CEF on the device if it has been disabled.</td>
</tr>
</tbody>
</table>
### Defining VPNs

Beginning in privileged EXEC mode, follow these steps to define VPN routing instances on the PE router:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>ip routing</td>
<td>Enable IP routing (required only if routing is disabled).</td>
</tr>
<tr>
<td>ip vrf vrf-name</td>
<td>Enter VRF configuration mode, and define the VPN routing instance by assigning a VRF name.</td>
</tr>
<tr>
<td>rd route-distinguisher</td>
<td>Create a VRF table by specifying a route distinguisher. Enter either an AS number and an arbitrary number (xxx:y) or an IP address and arbitrary number (A.B.C.D:y).</td>
</tr>
</tbody>
</table>

Repeat these steps for every PE router in the network and the appropriate interfaces until all routers and connected interfaces are enabled for MPLS.

Use the `no mpls ip` global configuration command to disable MPLS on the switch. Use the `no mpls label protocol ldp` global configuration command to return to the default TDP.
Chapter 44  Configuring MPLS, MPLS VPN, MPLS OAM, and EoMPLS

Configuring MPLS VPNs

Configuring BGP Routing Sessions

Beginning in privileged EXEC mode, follow these steps on the provider-edge router to configure BGP routing sessions in a provider network:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip routing</td>
</tr>
<tr>
<td></td>
<td>Enable IP routing (required only if routing is disabled).</td>
</tr>
<tr>
<td>Step 3</td>
<td>router bgp autonomous-system-number</td>
</tr>
<tr>
<td></td>
<td>Enable a BGP routing process, assign it the AS number passed to the other BGP routers, and enter router configuration mode. The AS number can be from 1 to 65535, with 64512 to 65535 designated as private autonomous numbers.</td>
</tr>
<tr>
<td>Step 4</td>
<td>neighbor {ip-address</td>
</tr>
<tr>
<td></td>
<td>Specify a neighbor IP address or BGP peer group that identifies it to the local autonomous system. The AS number can be from 1 to 65535.</td>
</tr>
<tr>
<td>Step 5</td>
<td>neighbor ip-address activate</td>
</tr>
<tr>
<td></td>
<td>Activate the advertisement of the IPv4 address family.</td>
</tr>
<tr>
<td>Step 6</td>
<td>end</td>
</tr>
<tr>
<td></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 7</td>
<td>show ip bgp neighbor</td>
</tr>
<tr>
<td></td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td>Step 8</td>
<td>copy running-config startup-config</td>
</tr>
<tr>
<td></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Use the no router bgp autonomous-system global configuration command to delete the BGP routing session.
Configuring Provide-Edge-to-Provider-Edge Routing Sessions

Beginning in privileged EXEC mode, follow these steps on the provider-edge router to configure a PE-to-PE routing session in a provider network that uses IBGP:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>router bgp autonomous-system-number</td>
</tr>
<tr>
<td></td>
<td>Enter router configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>address-family vpnv4 [unicast]</td>
</tr>
<tr>
<td></td>
<td>Enter address family configuration mode to configure routing sessions that use standard VPNv4 address prefixes. (Optional) unicast—Specify VPNv4 unicast address prefixes.</td>
</tr>
<tr>
<td>Step 4</td>
<td>neighbor ip-address remote-as as-number</td>
</tr>
<tr>
<td></td>
<td>Define an IBGP session between the provider-edge routers.</td>
</tr>
<tr>
<td>Step 5</td>
<td>neighbor ip-address activate</td>
</tr>
<tr>
<td></td>
<td>Activate the advertisement of the IPv4 address family.</td>
</tr>
<tr>
<td>Step 6</td>
<td>end</td>
</tr>
<tr>
<td></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 7</td>
<td>show ip bgp [ipv4] [neighbors] [vpnv4]</td>
</tr>
<tr>
<td></td>
<td>Verify BGP configuration. Display information about all BGP IPv4 prefixes.</td>
</tr>
<tr>
<td>Step 8</td>
<td>copy running-config startup-config</td>
</tr>
<tr>
<td></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Use the `no router bgp autonomous-system` global configuration command to delete the BGP routing session.

Configuring BGP Provider-Edge-to- Customer-Edge Routing Sessions

Beginning in privileged EXEC mode, follow these steps on the provider-edge router to configure a BGP PE-to-CE routing session:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>router bgp autonomous-system-number</td>
</tr>
<tr>
<td></td>
<td>Configure the BGP routing process with the AS number passed to other BGP routers, and enter router configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>address-family ipv4 [unicast] vrf vrf-name</td>
</tr>
<tr>
<td></td>
<td>Define EPG parameters for PE-to-CE routing sessions, and enter VRF address-family configuration mode. <strong>Note</strong> The default is off for auto-summary and synchronization in the VRF address-family configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>neighbor address remote-as as-number</td>
</tr>
<tr>
<td></td>
<td>Define an EBGP session between PE and CE routers.</td>
</tr>
<tr>
<td>Step 5</td>
<td>neighbor address activate</td>
</tr>
<tr>
<td></td>
<td>Activate the advertisement of the IPv4 address family.</td>
</tr>
<tr>
<td>Step 6</td>
<td>end</td>
</tr>
<tr>
<td></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 7</td>
<td>show ip bgp [ipv4] [neighbors]</td>
</tr>
<tr>
<td></td>
<td>Verify BGP configuration. Display information about all BGP IPv4 prefixes.</td>
</tr>
<tr>
<td>Step 8</td>
<td>copy running-config startup-config</td>
</tr>
<tr>
<td></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Use the `no router bgp as-number` global configuration command to delete the BGP routing session.
Configuring RIP Provider-Edge-to-Customer-Edge Routing Sessions

You can also use the OSPF routing protocol for PE-to-CE routing sessions.

Beginning in privileged EXEC mode, follow these steps on the provider-edge router to configure RIP PE-to-CE routing:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 router rip</td>
<td>Enable RIP routing, and enter router configuration mode.</td>
</tr>
<tr>
<td>Step 3 address-family ipv4 [unicast] vrf -name</td>
<td>Define RIP parameters for PE-to-CE routing sessions, and enter VRF address-family configuration mode.</td>
</tr>
<tr>
<td>Step 4 network prefix</td>
<td>Enable RIP on the PE-to-CE link.</td>
</tr>
<tr>
<td>Step 5 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 6 show ip rip database [network-prefix]</td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td>Step 7 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Use the no router rip global configuration command to disable RIP routing.

Configuring Static Route Provider-Edge-to-Customer-Edge Routing Sessions

Beginning in privileged EXEC mode, follow these steps on the provider-edge router to configure static routing:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 ip route vrf vrf-name prefix mask</td>
<td>Define the VRF static routing table to use for PE-to-CE sessions.</td>
</tr>
<tr>
<td>Step 3 router bgp autonomous-system-number</td>
<td>Enter the BGP routing process AS number, and enter router configuration mode.</td>
</tr>
<tr>
<td>Step 4 address-family ipv4 [unicast] vrf vrf-name</td>
<td>Define static route parameters for every PE-to-CE routing session, and enter VRF address-family configuration mode.</td>
</tr>
<tr>
<td></td>
<td>The default is off for auto-summary and synchronization in the VRF address-family configuration mode.</td>
</tr>
<tr>
<td>Step 5 redistribute static</td>
<td>Redistribute VRF static routes into the VRF BGP table.</td>
</tr>
<tr>
<td>Step 6 redistribute connected</td>
<td>Redistribute directly connected networks into the VRF BGP table.</td>
</tr>
<tr>
<td>Step 7 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 8 show ip bgp [ipv4]</td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td>Step 9 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
Packet Flow in an MPLS VPN

Figure 44-3 is an example of packet flow between two customer sites in an MPLS VPN network.

A customer (Fast Ethernet) port on switch PE1 is configured for routed operation in a VPN. The port uses static routing or a routing protocol (RIP, OSPF, EIGRP, or BGP) to forward packets. MP-BGP is configured over the PE1 switch ES port with a route distinguisher that is associated with the customer’s VPN. MP-BGP is configured to redistribute the routes and their associated VPN labels over the ES port that is using this route distinguisher.

The packet flow follows these steps:

---

**Step 1** Provider-edge switch PE1 (which could be a Catalyst 3750 Metro switch) receives a packet from the customer switch at site 1. The switch determines from the lookup table that the VRF is a VLAN running MPLS and uses the MPLS lookup table to determine what to do with the packet. The MPLS lookup table contains the peer LSR as the destination MAC address and the local interface as the source MAC address.

**Step 2** PE1 finds a BGP route with the appropriate next hop and labels, adds the appropriate labels to the packet, and forwards the packet out of the ES port to the next hop router (P3).

**Step 3** The P3 router receives the packet and forwards it over the MPLS-VPN network, based on the packet’s top label—the interior gateway protocol (IGP) label—and then removes the top label.

**Step 4** PE3 receives the packet, removes the MPLS encapsulation, and forwards the packet by using the VRF interface associated with the VPN label contained in the packet that has the customer-edge switch CE2 as the destination.
Understanding MPLS Traffic Engineering and Fast Reroute

This section describes the Catalyst 3750 Metro support of MPLS traffic engineering (TE) and includes these sections:

- MPLS TE, page 44-13
- MPLS TE Fast Reroute, page 44-14
- MPLS TE Primary and Backup Autotunnel, page 44-15

MPLS TE

MPLS traffic engineering (TE) provides control over how traffic is routed through the network. This increases the bandwidth efficiency by preventing over-use of some links while other links are under used. TE overrides the shortest path selected by the Interior Gateway Protocol (IGP) to select the most efficient path for traffic. Network resources are advertised by using a link-state routing protocol, such as Intermediate System-to-Intermediate System (IS-IS) or Open Shortest Path First (OSPF). MPLS TE then uses a unidirectional LSP or tunnel to forward traffic, calculating the tunnel paths based on required and available resources.

Regular MPLS traffic engineering automatically establishes and maintains label-switched paths (LSPs) across the backbone using Resource Reservation Protocol (RSVP). The path used by a given LSP is based on the LSP resource requirements and available network resources such as bandwidth. Available resources are flooded via extensions to the link-state based IGP.

For more information on MPLS TE, see this URL:


Paths for LSPs are calculated at the LSP headend, the first router in the LSP path. Under failure conditions, the headend determines a new route for the LSP based on destination, bandwidth, link attributes, and priority. RSVP-TE then establishes and maintains the TE tunnel across the MPLS backbone network. Packets are switched inside the tunnel by using MPLS labels. Recovery at the headend provides for the optimal use of resources.

The switch supports 250 tunnels in the TE headend and 2,000 tunnels at the midpoint.

The Catalyst 3750 Metro switch supports these MPLS TE features:

- OSPF, IS-IS, and RSVP extensions to support MPLS TE
- TE autotunnel primary and backup
- TE tunnel reoptimization to improve overall efficiency by rerouting some traffic trunks to new paths
- TE load sharing to a destination over paths with unequal costs. The switch supports up to 256 load-shared routes (load-shared routes for up to 256 destinations). Any additional load-balanced routes are forwarded in one path in the hardware.
- TE IP explicit address exclusion to exclude a link or node from the path. You use the `ip explicit-path` global configuration mode to enter explicit-path configuration mode and then use the `exclude-address` command to specify addresses to exclude from the path.
- Support for LDP over TE tunnels for Layer 3 VPN traffic by entering the `mpls ip` interface configuration command on the tunnel interface. The switch does not support LDP over TE tunnels for Layer 2 VPN traffic.
- Traffic forwarding to the TE tunnel using static routing
• TE autoroute, which installs the routers announced by the tailend router and the downstream routers into the routing table of the headend router. All traffic directed to prefixes beyond the tunnel end are pushed into the tunnel.

The Catalyst 3750 Metro switch does not support these MPLS TE features:
• Interarea TE support for OSPF and IS-IS
• TE path protection
• Shared risk link group (SRLG)
• Traffic forwarding to the TE tunnel using policy routing
• Traffic forwarding to the TE tunnel using forwarding adjacency
• Auto bandwidth
• Autotunnel mesh group

MPLS TE Fast Reroute

With MPLS TE, when a link or node failure occurs, the LSP headend determines a new route for the LSP. However, due to messaging delays, the headend cannot recover as quickly as making a repair at the point of failure. Fast reroute (FRR) protects the LSPs from link and node failures by locally repairing the LSP at the point of failure, allowing data to continue to flow while the headend routers establish replacement end-to-end LSPs. Fast reroute locally repairs the protected LSP by rerouting all LSP traffic crossing a failed link over backup tunnels that bypass the failed link or node.

- Link protection is also referred to as next hop (N-Hop) protection because the new route terminates at the next hop beyond the LSP failure.
- Node protection is also referred to as next-next-hop (NN-Hop) protection because the new route bypasses the next hop node and terminates at the node following the next-hop node. Node protection also provides protection from link failures because traffic bypasses the failed link and the failed node.

For more information about MPLS TE fast reroute, see this feature module:

The reroute decision is completely controlled locally by the router interfacing the failed link. The headend of the tunnel is also notified of the link failure through the IGP or through RSVP; the headend then attempts to establish a new LSP that bypasses the failure.

Local reroute prevents any further packet loss caused by the failed link. If the tunnel is configured to be dynamic, the headend of the tunnel then has time to reestablish the tunnel along a new, optimal route. If the headend still cannot find another path to take, it continues to use the backup tunnel.

Fast link change detection (FLCD) and RSVP hello messages form the failure detection mechanism. FLCD is notified when an interface encounters a link status change and RSVP hello enables the RSVP nodes to detect when a neighboring node is not reachable. You can configure RSVP hello messages by entering the \texttt{ip rsvp signalling hello [fast reroute] refresh} global configuration command.

Backup tunnels have these characteristics on the Catalyst 3750 Metro switch:
• A backup tunnel can protect multiple LSPs.
• When the primary tunnel restores, traffic changes from the backup tunnel back to the primary tunnel.
The switch does not support backup tunnel bandwidth protection.

The switch supports MPLS TE fast reroute over only routed ports and not over SVIs or EtherChannels.

**MPLS TE Primary and Backup Autotunnel**

The primary and backup autotunnel feature enables a switch to dynamically build backup tunnels and to dynamically create one-hop primary tunnels on all interfaces configured for MPLS TE.

- **Primary autotunnel** dynamically creates one-hop primary tunnels on all MPLS TE interfaces. Instead of configuring an MPLS TE tunnel with fast-reroute, you enter the `mpls traffic-eng auto-tunnel primary onehop` global configuration command to dynamically create one-hop tunnels on all MPLS TE interfaces.

- **Backup autotunnel** enables a router to dynamically build backup tunnels when they are needed so that you do not need to configure them manually. To configure backup autotunnel, enter the `mpls traffic-eng auto-tunnel backup router` configuration command.

---

**Configuring MPLS Traffic Engineering and Fast Reroute**

This section includes this information about configuring MPLSTE on a Catalyst 3750 Metro switch:

- Default MPLS TE and Fast Reroute Configuration, page 44-15
- MPLS TE and Fast Reroute Configuration Guidelines, page 44-15

These sections describe the configuration procedures:

- Configuring MPLS TE, page 44-16
- Configuring TE Fast Reroute, page 44-18
- Configuring Primary and Backup Autotunnels, page 44-20

---

**Default MPLS TE and Fast Reroute Configuration**

MPLS TE and fast reroute are not configured.

Backup or primary autotunnel is not configured.

---

**MPLS TE and Fast Reroute Configuration Guidelines**

Follow these guidelines when configuring MPLS TE:

- Not all of the MPLS TE commands that are visible in the switch command-line interface help are supported. See the “MPLS” section on page C-12 of Appendix C, “Unsupported Commands in Cisco IOS Release 12.2(55)SE.”

- To configure MPLS traffic engineering and fast reroute, the network must be running IP Cisco Express Forwarding (CEF) and MPLS and support at least one of these protocols: OSPF or IS-IS.

- For information on all MPLS commands, see the MPLS command reference at this URL: http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html
Configuring MPLS TE

For more information on MPLS TE, see this URL:

Beginning in privileged EXEC mode, follow these steps to configure MPLS TE and configure an interface to support RSVP-based tunnel signalling and IGP flooding:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip cef distributed</td>
</tr>
<tr>
<td>Step 3</td>
<td>mpls traffic-eng tunnels</td>
</tr>
<tr>
<td>Step 4</td>
<td>ip rsvp signalling hello</td>
</tr>
<tr>
<td>Step 5</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 6</td>
<td>mpls traffic-eng tunnels</td>
</tr>
<tr>
<td>Step 7</td>
<td>ip rsvp bandwidth bandwidth</td>
</tr>
<tr>
<td>Step 8</td>
<td>ip rsvp signalling hello</td>
</tr>
<tr>
<td>Step 9</td>
<td>end</td>
</tr>
<tr>
<td>Step 10</td>
<td>show mpls traffic-eng tunnel</td>
</tr>
<tr>
<td>Step 11</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

Enter `no mpls traffic-eng tunnels` to disable MPLS traffic engineering tunnels on the switch or interface. Enter the `no rsvp bandwidth` interface configuration command to return to the default.

Configuring an MPLS TE Tunnel

Beginning in privileged EXEC mode, follow these steps to configure an MPLS traffic engineering tunnel. The configured tunnel has two path setup options—a preferred explicit path and a backup dynamic path.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface tunnel tunnel-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>ip unnumbered loopback0</td>
</tr>
<tr>
<td>Step 4</td>
<td>tunnel destination A.B.C.D</td>
</tr>
<tr>
<td>Step 5</td>
<td>tunnel mode mpls traffic-eng</td>
</tr>
</tbody>
</table>
**Configuring MPLS Traffic Engineering and Fast Reroute**

**Step 6**

**Command**: `tunnel mpls traffic-eng bandwidth bandwidth`  
**Purpose**: Configure the bandwidth, in kb/s per second, set aside for the MPLS traffic engineering tunnel. The range is from 1 to 4294967295 kb/s. The default is 0.

**Step 7**

**Command**: `tunnel mpls traffic-eng path-option 1 explicit name name`  
**Purpose**: Configure a named IP explicit path.

**Step 8**

**Command**: `tunnel mpls traffic-eng path-option 2 dynamic`  
**Purpose**: Configure a backup path to be dynamically calculated from the traffic engineering topology database.

**Step 9**

**Command**: `exit`  
**Purpose**: Return to global configuration mode.

**Step 10**

**Command**: `ip explicit-path name name`  
**Purpose**: Specify the IP explicit path name, and enter IP explicit path configuration mode. An IP explicit path is a list of IP addresses, each representing a node or link in the explicit path.

**Step 11**

**Command**: `next-address A.B.C.E`  
**Purpose**: Specify the next IP address in the explicit path.

**Step 12**

**Command**: `next-address A.B.C.F`  
**Purpose**: Specify the second IP address in the explicit path.

**Step 13**

**Command**: `exclude-address A.B.C.X`  
**Purpose**: (Optional) Exclude an address from the IP explicit path.

**Step 14**

**Command**: `end`  
**Purpose**: Return to privileged EXEC mode.

**Step 15**

**Command**: `show ip explicit-paths`  
**Purpose**: Verify the configuration.

**Step 16**

**Command**: `copy running-config startup-config`  
**Purpose**: (Optional) Save your entries in the configuration file.

Enter the `no` forms of the commands to remove the configured MPLS tunnels. Enter the `no ip explicit-path name` global configuration command to disable IP explicit paths.

---

**Configuring the Routing Protocol for MPLS TE**

Beginning in privileged EXEC mode, follow these steps to configure IS-IS or OSPF for MPLS traffic engineering:

**Step 1**

**Command**: `configure terminal`  
**Purpose**: Enter global configuration mode.

**Step 2**

**Command**: `router {isis | ospf}`  
**Purpose**: Enable IS-IS or OSPF routing, and enter router configuration mode.

**Step 3**

**Command**: `mpls traffic-eng level 1`  
**Purpose**: Turn on MPLS traffic engineering for IS-IS level 1.

**Step 4**

**Command**: `mpls traffic-eng area 0`  
**Purpose**: Turn on MPLS traffic engineering for OSPF.

**Step 5**

**Command**: `mpls traffic-eng router-id loopback0`  
**Purpose**: Specify the traffic engineering router identifier for the node to be the IP address associated with interface loopback0.

**Step 6**

**Command**: `metric-style wide`  
**Purpose**: Configure a router to generate and accept only new-style stands for type, length, and value objects (TLVs).

**Note**: This command is for IS-IS routing only.

**Step 7**

**Command**: `end`  
**Purpose**: Return to privileged EXEC mode.

**Step 8**

**Command**: `show mpls traffic-eng`  
**Purpose**: Verify the configuration.

**Step 9**

**Command**: `show ip ospf mpls traffic-eng`  
**Purpose**: Verify the configuration.

**Step 10**

**Command**: `copy running-config startup-config`  
**Purpose**: (Optional) Save your entries in the configuration file.
To remove the traffic engineering router identifier, use the `no mpls traffic-eng router-id` command.

## Configuring TE Fast Reroute

Before or after entering the commands described in these procedures, you must enable the MPLS traffic engineering tunnel capability globally on the tunnel routers by entering the `mpls traffic-eng tunnels` global and interface configuration commands. For information about the commands for MPLS TE fast reroute, see this URL:


Beginning in privileged EXEC mode, follow these steps to enable MPLS traffic engineering fast reroute on an MPLS tunnel and to create a backup tunnel to the next hop or next-next hop:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>interface tunnel tunnel-number</code></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>ip unnumbered interface-id</code></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>tunnel destination A.B.C.D</code></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>tunnel mode mpls traffic-eng</code></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>`tunnel mpls traffic-eng path-option number {dynamic</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><code>tunnel mpls traffic-eng fast-reroute</code></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><code>ip explicit-path name path-name</code></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td><code>next-address A.B.C.E</code></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>Repeat Step 8 for additional IP addresses in the path.</td>
</tr>
</tbody>
</table>
Configuring MPLS Traffic Engineering and Fast Reroute

Enter the `no tunnel mode mpls traffic-eng global` configuration command to disable MPLS traffic engineering or the `no ip explicit-path` global configuration command to remove the IP explicit path configuration.

Configuring a Protected Link to Use a Backup Tunnel

Beginning in privileged EXEC mode, follow these steps to configure a protected link to use the backup tunnel:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>mpls traffic-eng backup-path tunnel tunnel-id</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
</tr>
<tr>
<td>Step 5</td>
<td>show mpls traffic-eng fast-reroute database</td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To remove the backup tunnel configuration, enter the `no mpls traffic-eng backup-path tunnel` interface configuration command.

Configuring Fast Reroute Failure Detection

Beginning in privileged EXEC mode, follow these steps to configure fast reroute failure detection:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip rsvp signalling hello</td>
</tr>
<tr>
<td>Step 3</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 4</td>
<td>ip rsvp signalling hello fast-reroute refresh misses number</td>
</tr>
</tbody>
</table>
Step 5: 
```
ip rsvp signalling hello fast-reroute refresh interval interval-value
```
Configure the frequency, in milliseconds, at which a node sends hello messages to a neighbor. Valid values are from 10 to 30000 (.01 to 30 seconds). The default frequency is 1000 milliseconds (10 seconds).

**Note** To prevent false detection of a down neighbor and unnecessarily triggering fast reroute, we recommend configuring a minimum frequency of 200 ms.

Step 6: 
```
ip rsvp signalling hello
```
Enable Hello signalling on the interface.

Step 7: 
```
end
```
Return to privileged EXEC mode.

Step 8: 
```
show ip rsvp fast-reroute
show ip rsvp hello instance summary
```
Verify the configuration.

Step 9: 
```
copy running-config startup-config
```
(Optional) Save your entries in the configuration file.

---

### Configuring Primary and Backup Autotunnels

The Autotunnel Primary and Backup feature enables a router to dynamically build backup tunnels and to dynamically create one-hop primary tunnels on all interfaces configured for MPLS TE. For information about the commands for MPLS autotunnel, see this URL:


Beginning in privileged EXEC mode, follow these steps to automatically create primary tunnels to all next hop neighbors:

---

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>mpls traffic-eng auto-tunnel primary onehop</td>
</tr>
<tr>
<td>Step 3</td>
<td>mpls traffic-eng auto-tunnel primary tunnel-num [min num] [max num]</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>mpls traffic-eng auto-tunnel primary timers removal rerouted sec</td>
</tr>
<tr>
<td>Step 5</td>
<td>mpls traffic-eng auto-tunnel primary config unnumbered interface-id</td>
</tr>
</tbody>
</table>
### Understanding MPLS OAM

MPLS OAM helps service providers monitor label-switched paths (LSPs) and quickly isolate MPLS forwarding problems to assist with fault detection and troubleshooting in an MPLS network. The Catalyst 3750 Metro switch supports these MPLS OAM features:

- LSP ping/traceroute LDP IPv4 version 3
- Any Transport over MPLS (AToM) Virtual Circuit Connection Verification (VCCV) to use MPLS LSP Ping to test the pseudowire section of an AToM virtual circuit (VC).

#### Step-by-Step Configuration

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: <code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2: <code>mpls traffic-eng auto-tunnel backup</code></td>
<td>Configure the switch to automatically create next-hop (NHOP) and next-next hop (NNHOP) backup tunnels.</td>
</tr>
<tr>
<td>Step 3: <code>mpls traffic-eng auto-tunnel backup nhop-only</code></td>
<td>Configure the switch to automatically build only next-hop (NHOP) backup tunnels.</td>
</tr>
<tr>
<td>Step 4: <code>mpls traffic-eng auto-tunnel backup timers removal unused sec</code></td>
<td>Configure how frequently (in seconds) a timer scans the backup autotunnels and removes tunnels that are not being used. Valid values are 0 to 604800. The default is every 3600 seconds (60 minutes).</td>
</tr>
<tr>
<td>Step 5: <code>mpls traffic-eng auto-tunnel backup config unnumbered interface interface-id</code></td>
<td>Enable IP processing without an explicit address. <code>interface interface-id</code> is the interface on which IP processing will be enabled without an explicit address. The default interface is Loopback0.</td>
</tr>
<tr>
<td>Step 6: <code>mpls traffic-eng auto-tunnel primary config mpls ip</code></td>
<td>Enable Label Distribution Protocol (LDP) on primary autotunnels.</td>
</tr>
<tr>
<td>Step 7: <code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 8: <code>show interface tunnel tunnel-num</code></td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td>Step 9: <code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Enter the **no** form of each command to delete the tunnel or disable the feature or capability. To remove all primary autotunnels, enter the **clear mpls traffic-eng auto-tunnel primary** privileged EXEC command.

Beginning in privileged EXEC mode, follow these steps to establish MPLS backup auto tunnels:
• IP Service Level Agreements (IP SLAs) to monitor MPLS LSP networks and IP SLAs Health Monitor to automatically generate LSP ping and traceroute to BGP VPN neighbors.

**Note**  
In Cisco IOS Release 12.2(37)SE, IP SLAs support implemented nonstandard IP SLAs command-line interface commands, using the `rtr` global configuration command to put the switch into response time reporter (RTR) configuration mode. Beginning with Cisco IOS Release 12.2(40)SE, the switch uses the standard IP SLAs configuration commands, using the `ip sla` global configuration command to put the switch into IP SLAs configuration mode. See Chapter 41, “Configuring Cisco IOS IP SLAs Operations,” for more information on configuring IP SLAs.

For more information about MPLS OAM, see the [MPLS LSP Ping/Traceroute for LDP/TE, and LSP Ping for VCCV feature guide](http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/ht_lspng.html) at this URL:


**Note**  
The switch does not support all of the commands referenced in the MPLS LSP Ping/Traceroute feature module. For a list of commands that are visible in the CLI help, but not supported on the switch, see Appendix C, “Unsupported Commands in Cisco IOS Release 12.2(55)SE.”

Beginning with Cisco IOS Release 12.2(40)SE, the switch supports these additional keywords for the `ping mpls` and `traceroute mpls` privileged EXEC commands to support RFC4379:

• Entering the `dsmap` keyword with the `ttl` keyword to the `ping` command allows you configure a MPLS echo request from the source router to expire at a transit router with a wildcard downstream map to obtain downstream information from the transit router.

• Entering the `flags fec` keyword configures the source router to force the transit router to validate the target forwarding equivalence class (FEC).

• Entering the `force-explicit-null` keyword adds a Null label to the end of the label stack to allow the destination provider-edge device to distinguish between traffic that has been rejected by the destination provider router and traffic that arrives untagged.

• Entering the `interval` keyword allows you to specify the echo request packet send interval.

• Entering the `output interface interface-id` keywords provides path information as input to the LDP IPv4 ping and traceroute configuration to force echo packets through the same paths for more detailed analysis for LSP debugging.

• Entering the `repeat` keyword specifies the number of retries attempted if an echo request times out before an echo reply is received.

• To allow interoperability between these IETF RFC 4379 drafts, the `revision` keyword was added to enable Cisco IOS releases to support the existing draft changes and any changes from future versions of the IETF LSP Ping draft. The switch supports revision 2 and RFC 4329 Compliant.

In addition, these other features have been added:

• Echo request return codes have been enhanced for better fault isolation.

• You can use the `no mpls oam` global configuration command to disable the MPLS OAM subsystem when MPLS is running.

• You can configure the maximum number of labels in a label stack for load balancing.
Understanding MPLS OAM

- The switch now supports LSP tree trace, using the `trace mpls multipath` privileged EXEC command to trace all possible paths of an LSP network between the ingress and egress routers by using downstream mapping.

Enhancements to the IP SLAs MPLS LSP Health Monitor include:

- Entering the `auto ip sla mpls-lsp-monitor` global configuration command automatically configures ping and traceroute boundaries
- Entering the `path-discover` command in auto IP SLA MPLS parameter configuration mode configures equal cost multipath (ECMP) tree trace. VPN end points are automatically discovered and ping or traceroute actions are automatically generated for each provider edge router.
- For more information on configuring the LSP Health Monitor, go to this URL: http://www.cisco.com/en/US/docs/ios/12_2sx/12_2sxh/feature/guide/sxh_hmon.html

LSP Ping

MPLS LSP ping uses MPLS echo request and reply packets, similar to Internet Control Message Protocol (ICMP) echo request and reply messages, to validate an LSP. ICMP echo request and reply messages validate IP networks; MPLS OAM echo and reply messages validate MPLS LDP networks. The LSP ping and trace functions use IPv4 UDP packets with UDP port number 3503. You can use MPLS LSP ping to validate IPv4 LDP or Forwarding Equivalence Classes (FECs) by using the `ping mpls` privileged EXEC command. The MPLS echo request packet is sent to a target router by using the label stack associated with the FEC to be validated.

The source address of the LSP echo request is the IP address of the LDP router generating the LSP request. The destination IP address is a 127.x.y.z/8 address, which prevents the IP packet from being switched to its destination if the LSP is broken. The 127.0.0.x destination address range prevents the OAM packets from exiting the egress provider-edge router, which keeps them from leaking from the service-provider network to the customer network.

In response to an MPLS echo request, an MPLS echo reply is forwarded as an IP packet by using IP, MPLS, or a combination of both. The source address of the MPLS echo-reply packet is an address obtained from the router generating the echo reply. The destination address is the source address of the router that originated the MPLS echo-request packet. The MPLS echo-reply destination port is the echo-request source port.

LSP Traceroute

MPLS LSP traceroute also uses MPLS echo request and reply packets to validate an LSP. You can use MPLS LSP traceroute to validate LDP IPv4 by using the `trace mpls` privileged EXEC command. The traceroute time-to-live (TTL) settings force expiration of the TTL along an LSP. MPLS LSP traceroute incrementally increases the TTL value in its MPLS echo requests (TTL = 1, 2, 3, 4) to discover the downstream mapping of each successive hop. The transit router processing the MPLS echo request returns an MPLS echo reply containing information about the transit hop in response to the TTL-expired MPLS packet. The MPLS echo reply destination port is sent to the echo request source port.
Understanding MPLS OAM

AToM VCCV (LSP Ping over Pseudowire)

You can use AToM VCCV control words to send control packets inband of an AToM pseudowire from the originating provider edge router or out-of-band by using router alert. The Catalyst 3750 Metro switch supports out-of-band VCCV. You configure this by using the `ping mpls pseudowire` privileged EXEC command. The transmission is intercepted at the destination provider-edge router, instead of being forwarded to the customer-edge router. You can use AToM VCCV and MPLS LSP ping to test the pseudowire section of AToM virtual circuits.

AToM VCCV consists of these components:

- A signaled component in which the AToM VCCV capabilities are advertised during virtual-circuit label signaling
- A switching component that causes the AToM VC payload to be treated as a control packet

An LSP ping through a Layer 2 pseudowire requires that the originating router first validate the pseudowire control channel capability during the exchange of virtual-circuit labels. In the Catalyst 3750 Metro switch, this is done by using a router alert label, which sends the LSP ping or traceroute packet to the egress PE router processor instead of forwarding it to the CE devices. This is type 2 AToM VCCV. The switch does not support inband VCCV validation using a control word (type 1).

IP SLAs Interworking with MPLS OAM

IP SLAs provides a way to generate MPLS LSPs and measure statistics between provider-edge routers participating in the MPLS network. It uses LSP ping and traceroute to determine network availability or measure network connectivity and performance between the provider-edge routers. You can manually configure IP SLAs LSP ping or traceroute, or you can configure it using the IP SLAs Health Monitor.

- When you manually configure LSP ping or traceroute, you explicitly specify the FEC you want to validate, for example, a VPN end point.
- When you use the MPLS LSP Health Monitor, you specify a VRF, and the monitor automatically discovers the VPN end points. When configured, the LSP Health Monitor automatically creates and deletes IP SLAs LSP ping or LSP traceroute operations based on network topology. It automatically discovers all adjacent BGP next-hop provider-edge routers and creates individual IP SLAs LSP ping operations for each applicable BGP next-hop neighbor.

For more information on configuring the LSP Health Monitor, go to this URL:


LSP Tree Trace and IP SLAs ECMP Tree Trace

As the number of MPLS deployments increases, the number of traffic types the MPLS networks carry could increase. In addition, load balancing in the MPLS network provides alternate paths for carrying MPLS traffic to a target router, making troubleshooting forwarding problems between PEs difficult. The MPLS LSP multipath tree trace feature provides the means to discover all possible routing paths of an LSP network between an egress and ingress router by using downstream mapping. Once discovered, you can retest these paths periodically by using MPLS LSP ping or traceroute. This feature is an extension to the MPLS LSP traceroute functionality for the tracing of LDP IPv4 LSPs.

With equal cost multipath (ECMP) tree trace, the source router tries to force the request down each ECMP path so that the targeted FEC crosses all possible ECMP paths. The source LSR starts path discovery by sending a transit router a bitmap in an MPLS echo request. The transit router returns
information that contains subsets of the bitmap in a downstream map in an echo reply. The source router uses the information in the echo reply to interrogate the next router. It interrogates each successive router until it finds one bitmap setting that is common to all routers along the path.

You can manually configure tree trace by using downstream mapping Type Length Values (TLVs). You can also use the ECMP tree trace feature in the IP SLAs LSP Health Monitor. When you enter the `path-discover` command in auto IP SLA MPLS parameter configuration mode, VPN end points are automatically discovered and ping or traceroute actions are automatically generated for each provider edge router. You can also use the LSP Health Monitor to configure multioperation scheduling.

For more information about LSP multipath tree trace, see this URL:

### Configuring MPLS OAM and IP SLAs MPLS

This section includes this information about configuring MPLS OAMs on a Catalyst 3750 Metro switch:

- Default MPLS OAM Configuration, page 44-25
- MPLS OAM Configuration Guidelines, page 44-25

These sections describe the optional or required tasks:

- Using LSP Ping for LDP IPv4 FEC, page 44-26
- Using LSP Traceroute for LDP IPv4 FEC, page 44-28
- Using LSP Ping for Pseudowire (AToM VCCV), page 44-29
- Configuring IP SLAs MPLS Ping and Traceroute, page 44-30
- Using LSP Tree Trace, page 44-36

### Default MPLS OAM Configuration

MPLS OAM LSP ping and traceroute are not configured.

The IP SLAs MPLS LSP Health Monitor is not configured.

The `mpls oam` global configuration command is enabled.

### MPLS OAM Configuration Guidelines

Follow these guidelines when configuring MPLS OAM:

- The switch does not support traffic engineering FEC in this release.
- Because MPLS OAM detects problems in the MPLS LSP network, it is a useful tool when there is a discrepancy between the MPLS LSP and IP networks or between the MPLS control plane and data plane.
- When the Catalyst 3750 Metro switch is used as a provider router in the core and ECMP tree trace is configured, the switch can force the LSP packet down only one path, the actual data path. This limitation applies only to the Catalyst 3750 Metro switch.
### Using LSP Ping for LDP IPv4 FEC

When you enter the `ping mpls` privileged EXEC command to begin an LSP ping operation, the keyword that follows specifies the Forwarding Equivalence Class (FEC) that is the target of the LCP ping to which you want to verify connectivity.

Beginning in privileged EXEC mode, follow these steps to configure LSP LDP IPv4 ping:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Configure LSP IPv4 ping. The keywords have these meanings:</strong></td>
</tr>
<tr>
<td>ping mpls ipv4</td>
<td><em>destination-address destination-mask</em>—Specify the address and network mask of the target FEC.</td>
</tr>
<tr>
<td></td>
<td><em>(Optional) destination address-start address-end increment</em> —Enter the destination 127 network address range.</td>
</tr>
<tr>
<td></td>
<td><em>(Optional) exp exp-bits</em>—Specify the MPLS experimental-field value in the MPLS header for an echo reply. The range is from 0 to 7. The default is 0.</td>
</tr>
<tr>
<td></td>
<td><em>(Optional) interval ms</em>—Specify the time in milliseconds between successive MPLS echo requests. The range is 0 to 3600000 ms; the default is 0.</td>
</tr>
<tr>
<td></td>
<td><em>(Optional) pad pattern</em>—Specify to use the pad TLV to fill the datagram so that the MPLS echo request is the specified size.</td>
</tr>
<tr>
<td></td>
<td><em>(Optional) repeat count</em>—Specify the number of times to resend the packet. The range is from 1 to 2147483647. If you do not enter the <code>repeat</code> keyword, the packet is sent 5 times.</td>
</tr>
<tr>
<td></td>
<td><em>(Optional) reply dscp dscp-value</em>—Specify a specific class of service (CoS) in an echo reply by providing a differentiated services code point (DSCP) value.</td>
</tr>
</tbody>
</table>
Chapter 44 Configuring MPLS, MPLS VPN, MPLS OAM, and EoMPLS

Configuring MPLS OAM and IP SLAs MPLS

This is an example of an LSP ping:

```
Switch# ping mpls ipv4 10.131.159.251/32 destination 127.0.0.1 127.0.0.2 0.0.0.1 repeat 2
sweep 1450 1475 25
```

This is an example of an LSP ping:

```
Switch# ping mpls ipv4 10.131.159.251/32 destination 127.0.0.1 127.0.0.2 0.0.0.1 repeat 2
sweep 1450 1475 25
```
# Using LSP Traceroute for LDP IPv4 FEC

The LSP traceroute originator sends incremental MPLS echo requests to discover the downstream mapping of each successive hop. When the originating provider edge router receives the reply from the intermediate router, it forms another MPLS echo request with the same target FEC and the time-to-live is incremented by one.

Beginning in privileged EXEC mode, follow these steps to configure LSP LDP IPv4 traceroute:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Configure LSP IPv4 traceroute. The keywords have these meanings:</td>
</tr>
<tr>
<td><strong>traceroute mpls ipv4</strong></td>
<td></td>
</tr>
<tr>
<td><em>destination-address destination-mask</em></td>
<td>Specify the address and network mask of the target FEC.</td>
</tr>
<tr>
<td><em>address-start address-end increment</em></td>
<td>Enter the destination 127 network address range.</td>
</tr>
<tr>
<td><em>[exp exp-bits]</em></td>
<td>Specify the MPLS experimental field value in the MPLS header for an echo reply. The range is from 0 to 7. The default is 0.</td>
</tr>
<tr>
<td><em>[reply dscp dscp-value]</em></td>
<td>Specify a specific class of service (CoS) in an echo reply by providing a differentiated services code point (DSCP) value.</td>
</tr>
<tr>
<td><em>reply mode</em></td>
<td>Specify the reply mode for the echo request packet. Enter <em>ipv4</em> to reply with an IPv4 UDP packet (the default) or <em>router-alert</em> to reply with an IPv4 UDP packet with router alert.</td>
</tr>
<tr>
<td><em>revision</em></td>
<td>Enter the draft revision number as 1, 2, or 3.</td>
</tr>
<tr>
<td><em>source source-address</em></td>
<td>Specify the source address or the name. This is the destination address in the MPLS echo response. The default address is looopback0.</td>
</tr>
<tr>
<td><em>timeout seconds</em></td>
<td>Specify the timeout interval for an MPLS request packet. The range is from 0 to 3600 seconds. The default is 2 seconds.</td>
</tr>
<tr>
<td><em>ttl time-to-live</em></td>
<td>Specify a time-to-live value. The range is from 1 to 255.</td>
</tr>
<tr>
<td><em>verbose</em></td>
<td>Display the MPLS echo reply sender address of the packet and return codes.</td>
</tr>
<tr>
<td><em>revision number</em></td>
<td>Enter a Cisco-TLV-revision-number, 1 through 4.</td>
</tr>
<tr>
<td><em>force-explicit-null</em></td>
<td>Add an explicit NULL label to the end of the label stack.</td>
</tr>
<tr>
<td><em>output interface interface-id</em></td>
<td>Specify the output interface for the echo request.</td>
</tr>
<tr>
<td><em>nexthop ip-address</em></td>
<td>Force packets to go through the specified next-hop address.</td>
</tr>
<tr>
<td><em>flags fec</em></td>
<td>Request FEC stack checking at the transit router.</td>
</tr>
</tbody>
</table>
This is an example of configuring an LSP traceroute:

```
Switch# traceroute mpls ipv4 10.131.159.251/32 destination 127.0.0.1 127.0.0.2 1 ttl5
```

### Using LSP Ping for Pseudowire (AToM VCCV)

Entering the `ping mpls pseudowire` privileged EXEC command invokes the functionality of MPLS VCCV, which is the ability to inject traffic control into an AToM virtual circuit and have it intercepted by the remote provider edge router instead of being passed to the attachment circuits for switching. The command requires you to enter the egress provider edge IP address and a virtual-circuit identifier.

Beginning in privileged EXEC mode, follow these steps to configure LSP ping over pseudowire:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Configure LSP ping over pseudowire. The keywords have these meanings:</td>
</tr>
<tr>
<td><code>ping mpls pseudowire ipv4-address vc-id</code></td>
<td></td>
</tr>
<tr>
<td><code>[destination start-address [end-address [address-increment]]] [exp exp-bits]</code></td>
<td></td>
</tr>
<tr>
<td>`[interval ms] [pad pattern] [repeat count] [reply dscp dscp-value] [reply mode {ipv4</td>
<td>router-alert}]`</td>
</tr>
<tr>
<td>`[revision {1</td>
<td>2</td>
</tr>
<tr>
<td><strong>Command</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>ping mpls pseudowire ipv4-address vc-id</code></td>
<td>Configure LSP ping over pseudowire. The keywords have these meanings:</td>
</tr>
<tr>
<td><code>[destination start-address [end-address [address-increment]]] [exp exp-bits]</code></td>
<td></td>
</tr>
<tr>
<td>`[interval ms] [pad pattern] [repeat count] [reply dscp dscp-value] [reply mode {ipv4</td>
<td>router-alert}]`</td>
</tr>
<tr>
<td>`[revision {1</td>
<td>2</td>
</tr>
</tbody>
</table>

- **ipv4-address** — Specify the IPv4 address of the peer.
- **vc-id** — Specify virtual-circuit identification number. The range is from 1 to 4294967295.
- **destination** — Enter the destination 127 network address or address range with increment.
- **exp exp-bits** — Specify the MPLS experimental-field value in the MPLS header. The range is from 0 to 7. The default is 0.
- **interval ms** — Specify the time in milliseconds between successive MPLS echo requests. The range is from 0 to 3600000; the default is 0.
- **pad pattern** — Specify that the pad TLV is used to fill the datagram so that the MPLS echo request is the specified size.
- **repeat count** — Specify the number of times to resend the packet. The range is from 1 to 2147483647. The default is 1. If you do not enter the `repeat` keyword, the same packet is sent 5 times.
- **reply dscp dscp-value** — Specify a specific class of service (CoS) in an echo reply by providing a differentiated services code point (DSCP) value.
- **reply mode {ipv4 | router-alert}** — Specify the reply mode for the echo request packet. Enter `ipv4` to reply with an IPv4 packet (the default) or `router-alert` to reply with an IPv4 UPD packet with router alert. Router alert is type 2 AToM VCCV.
- **revision** — Enter the IETF MPLS ping draft revision number as 1, 2, or 3.
- **size packet-size** — Specify the size of the packet with the label stack imposed as the number of bytes in each ping. The range is from 40 to 18024. The default is 100.
- **sweep minimum maximum size-increment** — Send a number of packets of different sizes.
This is an example of an LSP ping over pseudowire:

Switch# ping mpls pseudowire 10.131.159.251 22 127.0.0.1 127.0.0.2 1 exp 5

### Configuring IP SLAs MPLS Ping and Traceroute

To use IP SLAs for monitoring MPLS LSP ping or traceroute operations to monitor Layer 3 MPLS VPNs, you can manually configure the IP SLAs ping or trace operation or you can configure the IP SLAs LSP Health Monitor. When configured, the LSP Health Monitor automatically discovers VPN endpoints and creates and deletes IP SLAs ping or traceroute operations based on network topology.

As with any IP SLAs operation, you can schedule the start time and end time for MPLS IP SLAs ping or trace, as well as whether it is an ongoing or recurring operation. Multioperation scheduling support for the LSP Health Monitor feature provides the capability to easily schedule the automatically created operations to begin at intervals equally distributed over a specified duration of time (schedule period) and to restart at a specified frequency. Multioperation scheduling is particularly useful in cases where the LSP Health Monitor is enabled on a source PE router that has a large number of PE neighbors and, therefore, a large number of IP SLAs operations running at the same time.

This section includes these configuration procedures:

- Configuring the IP SLAs LSP Health Monitor, page 44-31
- Manually Configuring IP SLAs MPLS LSP Ping or Traceroute, page 44-34

For more details about LSP Health Monitor and MPLS IP SLAs ping or traceroute, see the IP SLAs- LSP Health Monitor feature module at this URL:


For more details about IP SLAs operations, see Chapter 44, “Configuring MPLS, MPLS VPN, MPLS OAM, and EoMPLS.” For detailed information about IP SLAs commands, see the command reference at this URL:

Configuring the IP SLAs LSP Health Monitor

You can configure the MPLS LSP Health Monitor to discover BGP VPN next hops and automatically create IP SLAs LSP ping or traceroute operations. You can specify an LSP ping or traceroute operation and VRF tables to be used. By default the LSP Health Monitor discovers all BGP next-hop neighbors by using all VRFs associated with the source provider edge router.

When you configure an LSP Health Monitor operation, you enter auto IP SLAs MPLS parameters configuration mode where you can configure the optional parameters shown in the Steps 4 through 17. See the IP SLAs-LSP Health Monitor feature module for more information about the parameters.

You must configure the MPLS LSP Health Monitor on a provider-edge router. The IP SLAs measurement statistics are stored on the source PE router.

Beginning in privileged EXEC mode, follow these steps to configure the operation parameters, reaction conditions, and scheduling options for a MPLS LSP monitor ping or traceroute.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>auto ip sla mpls-lsp-monitor operation-number</td>
<td>Specify an LSP Health Monitor operation number and enter auto IP SLA MPLS configuration mode. The operation number range is from 1 to 2147483647.</td>
</tr>
<tr>
<td>3</td>
<td>type {echo</td>
<td>pathEcho} {ipsla-vrf-all</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• echo—Select an LSP monitor ping operation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• pathEcho—Select an LSP monitor traceroute operation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ipsla-vrf-all—Configure IP SLAs MPSL LSP monitor for all VPNs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• vrf vpn-name—Configure the IP SLAs LSP monitor for the specified VPN.</td>
</tr>
<tr>
<td>4</td>
<td>access-list access-list-number</td>
<td>(Optional) Specify an access list to apply to LSP Health Monitor operation.</td>
</tr>
<tr>
<td>5</td>
<td>delete-scan-factor factor</td>
<td>(Optional) Specify the number of times the LSP Health Monitor checks the scan queue before automatically deleting IP SLAs operations for BGP next-hop neighbors that are no longer valid. The factor range is 0 to 2147483647. The default scan factor is 1.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note You must use the scan-interval command with this command.</td>
</tr>
<tr>
<td>6</td>
<td>exp exp-bits</td>
<td>(Optional) Specify the experimental field value in the echo request packet header. The range is 0 to 7; the default value is 0.</td>
</tr>
<tr>
<td>7</td>
<td>force-explicit-null</td>
<td>(Optional) Add an explicit null label to all echo request packets of an IP SLAs operation.</td>
</tr>
<tr>
<td>8</td>
<td>lsp-selector ip-address</td>
<td>(Optional) Specify the local host IP address used to select the IP SLAs operation LSP. The default is 127.0.0.1.</td>
</tr>
</tbody>
</table>
## Command Purpose

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td><code>reply-dscp-bits dscp-value</code></td>
<td>(Optional) Specify the differentiated services codepoint (DSCP) value for an echo reply packet of an IP SLAs operation. The default value is 0.</td>
</tr>
<tr>
<td>10</td>
<td>`reply-mode {ipv4</td>
<td>router-alert}`</td>
</tr>
<tr>
<td>11</td>
<td><code>request-data-size bytes</code></td>
<td>(Optional) Specify the protocol data size for an IP SLAs request packet. The range is 100 to 1500; the default is 100 bytes.</td>
</tr>
<tr>
<td>12</td>
<td><code>scan-interval minutes</code></td>
<td>(Optional) Specifies the time interval (in minutes) at which the LSP Health Monitor checks the scan queue for BGP next hop neighbor updates. The range is 1 to 70560; the default is 240 minutes.</td>
</tr>
<tr>
<td>13</td>
<td>`secondary-frequency {both</td>
<td>connection-loss</td>
</tr>
<tr>
<td>14</td>
<td><code>tag text</code></td>
<td>(Optional) Create a user-specified identifier for an IP SLAs operation.</td>
</tr>
<tr>
<td>15</td>
<td><code>threshold milliseconds</code></td>
<td>(Optional) Specify the rising threshold (hysteresis) that generates a reaction event and stores history information for an IP SLAs operation. The range is 0 to 2147483647; the default is 5000 ms.</td>
</tr>
<tr>
<td>16</td>
<td><code>timeout milliseconds</code></td>
<td>(Optional) Specify the amount of time that the IP SLAs operation waits for a response from its request packet. The range is 0 to 604800000; the default value is 5000 ms.</td>
</tr>
<tr>
<td>17</td>
<td><code>ttl time-to-live</code></td>
<td>(Optional) Specify the maximum hop count for an IP SLAs echo request packet. The range is 1 to 255.</td>
</tr>
<tr>
<td>18</td>
<td><code>exit</code></td>
<td>Exit IP SLAs MPLS LSP monitor path discover configuration mode and return to auto IP SLA MPLS parameter configuration mode.</td>
</tr>
<tr>
<td>19</td>
<td><code>exit</code></td>
<td>Exit auto IP SLA MPLS parameter configuration mode and returns to global configuration mode.</td>
</tr>
</tbody>
</table>
## Chapter 44  Configuring MPLS, MPLS VPN, MPLS OAM, and EoMPLS

### Configuring MPLS OAM and IP SLAs MPLS

#### Step 20
**auto ip sla mpls-lsp-monitor**

**reaction-configuration**  
*operation-number*  
*react*  
*monitored-element*  
*[action-type option]*  
*[threshold-type {consecutive [occurrences] | immediate | never}]*

(Optional) Configure other LSP Health Monitor actions:

- **operation-number**—Enter the operation number.
- **react monitored-element**—Specify the element to be monitored for violations. For example, enter **connectionLoss** to configure a reaction to a 1-way connection loss for the operation.
- **(Optional) action-type option**—Specify the action to take when the threshold event occurs. For example, enter **none** for no action or **trapOnly** to send an SNMP logging trap.
- **(Optional) threshold-type**—Specify when the action-type occurs. These are the options:
  - **consecutive [occurrences]**—When reaction conditions are met consecutively for a specified number of times. The valid range is from 1 to 16; the default is 5.
  - **immediate**—When the reaction conditions are met.
  - **never**—Never. This is the default threshold type.

#### Step 21
**auto ip sla mpls-lsp-monitor schedule**

*operation-number*  
*schedule-period*  
*seconds*  
*[frequency seconds]*  
*[start-time {hh:mm:ss}]*  
*[month day | day month]*  
*[pending | now | after hh:mm:ss]*

Schedule time parameters for the LSP Health Monitor.

- **operation number**—Enter the operation number.
- **schedule-period seconds**—Enter the schedule period in seconds. The range is 1 to 604800 seconds.
- **(Optional) frequency seconds**—Enter the frequency for LSP monitoring in seconds. The range is 1 to 604800 seconds.
- **(Optional) start-time**—Enter the time for the operation to begin collecting information:
  - To start at a specific time, enter the hour, minute, second (in 24-hour notation) and day of the month. If no month is entered, the default is the current month.
  - Enter **pending** to select no information being collected until a start time is selected.
  - Enter **now** to start the operation immediately.
  - Enter **after hh:mm:ss** to indicate that the operation should start after the entered time has elapsed.

#### Step 22
**auto ip sla mpls-lsp-monitor reset**

(Optional) Reset LDP monitor group statistics.

#### Step 23
**end**

Return to privileged EXEC mode.

#### Step 24
**show ip sla mpls-lsp-monitor configuration**  
*[operation-number]*

Show the configured LSP monitoring operations.

#### Step 25
**copy running-config startup-config**

(Optional) Save your entries in the configuration file.

#### Step 26
**show ip sla mpls-lsp-monitor summary**

Display a summary of IP SLAs LSP MPLS status.
Enter the `no auto ip sla mpls-lsp-monitor operation-number` global configuration command to delete the operation.

This is an example of configuring the MPLS LSP Health Monitor for all VPNs:

```
Switch# config t
Switch(config)# auto ip sla mpls-lsp-monitor 1
Switch(config-auto-ip-sla-mpls)# type echo ipsla-vrf-all
Switch(config-auto-ip-sla-mpls-params)# timeout 1000
Switch(config-auto-ip-sla-mpls-params)# scan-interval 1
Switch(config-auto-ip-sla-mpls-params)# secondary-frequency connection-loss 10
Switch(config-auto-ip-sla-mpls-params)# secondary-frequency timeout 10
Switch(config-auto-ip-sla-mpls-params)# exit
Switch(config)# auto ip sla mpls-lsp-monitor reaction-configuration 1 react connectionLoss
threshold-type consecutive 3 action-type trapOnly
Switch(config)# auto ip sla mpls-lsp-monitor schedule 1 schedule-period 60 start-time now
Switch(config)# end
```

### Manually Configuring IP SLAs MPLS LSP Ping or Traceroute

Beginning in privileged EXEC mode, follow these steps to manually configure the IP SLAs LSP ping or traceroute:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>ip sla operation-number</td>
<td>Enter an IP SLAs operation number and enter IP SLAs configuration mode. The range is from 1 to 214783647.</td>
</tr>
<tr>
<td>3</td>
<td>mpls lsp [ping</td>
<td>trace] ipv4 destination_address destination_mask [force-explicit-null] [lsp-selector ip_address] [reply dscp] [reply mode {ipv4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ping—Select an LSP monitor ping operation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• trace—Select an LSP monitor traceroute operation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• destination_address destination_mask—Enter the address and network mask of the target.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) force-explicit-null—Add an explicit NULL label to the end of the label stack.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) lsp-selector ip_address—Specify the local host address used to select the LSP.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) reply dscp dscp-value—Specify a specific class of service (CoS) in an echo reply by providing a differentiated services code point (DSCP) value.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) reply mode {ipv4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) source_ipaddr source_address—Specify the source IP address of the echo request originator.</td>
</tr>
<tr>
<td>4</td>
<td>exp exp-bits</td>
<td>(Optional) Specify the experimental field value in the echo request packet header. The range is 0 to 7; the default value is 0.</td>
</tr>
</tbody>
</table>
Configuring MPLS OAM and IP SLAs MPLS

Step 5  request-data-size bytes
(Optional) Specify the protocol data size for an IP SLAs request packet. The range is 100 to 1500; the default is 100 bytes.

Step 6  secondary-frequency { both | connection-loss | timeout } frequency
(Optional) Set the secondary frequency (faster measurement frequency) to which an IP SLAs operation should change when a reaction condition occurs. The frequency range is 1 to 604800.

Step 7  tag text
(Optional) Create a user-specified identifier for an IP SLAs operation.

Step 8  threshold milliseconds
(Optional) Specify the rising threshold (hysteresis) that generates a reaction event and stores history information for an IP SLAs operation. The range is 0 to 2147483647; the default is 5000 ms.

Step 9  timeout milliseconds
(Optional) Specify the amount of time that the IP SLAs operation waits for a response from its request packet. The range is 0 to 604800000; the default value is 5000 ms.

Step 10  ttl time-to-live
(Optional) Specify the maximum hop count for an IP SLAs echo request packet. The range is 1 to 255.

Step 11  exit
Return to global configuration mode.

Step 12  ip sla schedule operation-number [ ageout seconds ] [ life { forever | seconds } ] [ recurring ] [ start-time { hh:mm:ss [ month day | day month ] | pending | now | after hh:mm:ss } ]
Schedule the time parameters for MPLS LSP monitoring.
  • operation-number—Enter the IP SLAs operation number.
  • (Optional) ageout seconds—Enter the number of seconds to keep the operation in memory when it is not actively collecting information. The default is 0 seconds (never ages out). The range is 0 to 2073600 seconds.
  • (Optional) life—Set the operation to run indefinitely (forever) or for a specific number of seconds. The range is from 0 to 2147483647. The default is 3600 seconds (1 hour)
  • (Optional) recurring—Set the probe to be automatically scheduled every day.
  • (Optional) start-time—Enter the time for the operation to begin collecting information:
    – To start at a specific time, enter the hour, minute, second (in 24-hour notation) and day of the month. If no month is entered, the default is the current month.
    – Enter pending to select no information being collected until a start time is selected.
    – Enter now to start the operation immediately.
    – Enter after hh:mm:ss to indicate that the operation should start after the entered time has elapsed.

Step 13  end
Return to privileged EXEC mode.

Step 14  show ip sla configuration [ operation-number ]
Show the configured LSP monitoring operations.
Configuring MPLS OAM and IP SLAs MPLS

Chapter 44 Configuring MPLS, MPLS VPN, MPLS OAM, and EoMPLS

Configuring MPLS OAM and IP SLAs MPLS

### Configuring MPLS OAM and IP SLAs MPLS

To remove an IP SLAs operation, enter the no ip sla operation-number global configuration command.

This is an example of manually configuring an MPLS LSP ping operation:

```
Switch# config t
Switch(config)# ip sla 1
Switch(config-ip-sla)# mpls lsp ping ipv4 192.168.1.4 255.255.255.255 lsp-selector 127.1.1.1
Switch(config-ip-sla-lspPing)# secondary-frequency connection-loss 30
Switch(config-ip-sla-lspPing)# secondary-frequency timeout 30
Switch(config-ip-sla-lspPing)# exit
Switch(config)# ip sla schedule 1 start-time now life forever
Switch(config)# exit
```

Using LSP Tree Trace

LSP tree trace is the capability to trace through all possible paths of an LSP network between the ingress and egress routers by using downstream mapping. You can manually configure tree trace using the `trace mpls multipath` privileged EXEC command. You can use IP SLAs Health Monitor for (ECMP tree trace by entering the `path-discover` command in auto IP SLA MPLS parameter configuration mode. VPN end points are automatically discovered and ping or traceroute actions are automatically generated for each provider edge router.

This section includes these configuration procedures:

- Manually Setting LSP Tree Trace, page 44-36
- Configuring ECMP IP SLAs Tree Trace, page 44-37

### Manually Setting LSP Tree Trace

Beginning in privileged EXEC mode, follow these steps to manually set LSP tree trace:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** traceroute mpls multipath ipv4 destination-address destination-mask [destination address-start address-end increment] [exp exp-bits] [reply dscp dscp-value] [reply mode [ipv4 | router-alert]] [revision [1 | 2 | 3]] [source source-address] [timeout seconds] [ttl time-to-live] [verbose] [revision [1 | 2 | 3]] [force-explicit-null] [output interface interface-id [nexthop ip-address]] [flags fec] | Configure LSP LDP IPv4 traceroute. The keywords have these meanings:  
  - `destination-address destination-mask`—Specify the address and network mask of the target FEC.  
  - (Optional) `destination address-start address-end increment`—Enter the destination 127 network address range.  
  - (Optional) `exp exp-bits`—Specify the MPLS experimental field value in the MPLS header for an echo reply. The range is from 0 to 7. The default is 0.  
  - (Optional) `reply dscp dscp-value`—Specify a specific class of service (CoS) in an echo reply by providing a differentiated services code point (DSCP) value.  

To remove an IP SLAs operation, enter the no ip sla operation-number global configuration command.

This is an example of manually configuring an MPLS LSP ping operation:

```
Switch# config t
Switch(config)# ip sla 1
Switch(config-ip-sla)# mpls lsp ping ipv4 192.168.1.4 255.255.255.255 lsp-selector 127.1.1.1
Switch(config-ip-sla-lspPing)# secondary-frequency connection-loss 30
Switch(config-ip-sla-lspPing)# secondary-frequency timeout 30
Switch(config-ip-sla-lspPing)# exit
Switch(config)# ip sla schedule 1 start-time now life forever
Switch(config)# exit
```

**Command** | **Purpose**
--- | ---
**Step 1** traceroute mpls multipath ipv4 destination-address destination-mask [destination address-start address-end increment] [exp exp-bits] [reply dscp dscp-value] [reply mode [ipv4 | router-alert]] [revision [1 | 2 | 3]] [source source-address] [timeout seconds] [ttl time-to-live] [verbose] [revision [1 | 2 | 3]] [force-explicit-null] [output interface interface-id [nexthop ip-address]] [flags fec] | Configure LSP LDP IPv4 traceroute. The keywords have these meanings:  
  - `destination-address destination-mask`—Specify the address and network mask of the target FEC.  
  - (Optional) `destination address-start address-end increment`—Enter the destination 127 network address range.  
  - (Optional) `exp exp-bits`—Specify the MPLS experimental field value in the MPLS header for an echo reply. The range is from 0 to 7. The default is 0.  
  - (Optional) `reply dscp dscp-value`—Specify a specific class of service (CoS) in an echo reply by providing a differentiated services code point (DSCP) value.

Using LSP Tree Trace

LSP tree trace is the capability to trace through all possible paths of an LSP network between the ingress and egress routers by using downstream mapping. You can manually configure tree trace using the `trace mpls multipath` privileged EXEC command. You can use IP SLAs Health Monitor for (ECMP tree trace by entering the `path-discover` command in auto IP SLA MPLS parameter configuration mode. VPN end points are automatically discovered and ping or traceroute actions are automatically generated for each provider edge router.

This section includes these configuration procedures:

- Manually Setting LSP Tree Trace, page 44-36
- Configuring ECMP IP SLAs Tree Trace, page 44-37

**Manually Setting LSP Tree Trace**

Beginning in privileged EXEC mode, follow these steps to manually set LSP tree trace:

**Command** | **Purpose**
--- | ---
**Step 1** traceroute mpls multipath ipv4 destination-address destination-mask [destination address-start address-end increment] [exp exp-bits] [reply dscp dscp-value] [reply mode [ipv4 | router-alert]] [revision [1 | 2 | 3]] [source source-address] [timeout seconds] [ttl time-to-live] [verbose] [revision [1 | 2 | 3]] [force-explicit-null] [output interface interface-id [nexthop ip-address]] [flags fec] | Configure LSP LDP IPv4 traceroute. The keywords have these meanings:  
  - `destination-address destination-mask`—Specify the address and network mask of the target FEC.  
  - (Optional) `destination address-start address-end increment`—Enter the destination 127 network address range.  
  - (Optional) `exp exp-bits`—Specify the MPLS experimental field value in the MPLS header for an echo reply. The range is from 0 to 7. The default is 0.  
  - (Optional) `reply dscp dscp-value`—Specify a specific class of service (CoS) in an echo reply by providing a differentiated services code point (DSCP) value.
Beginning in privileged EXEC mode, follow these steps to use the LSP Health Monitor to configure IP SLAs ECMP tree trace:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><code>auto ip sla mpls-lsp-monitor operation-number</code></td>
<td>Specify an LSP Health Monitor operation number and enter auto IP SLAs MPLS configuration mode. The operation number range is from 1 to 2147483647.</td>
</tr>
<tr>
<td><code>path-discover</code></td>
<td>Enter IP SLAs MPLS LSP monitor path discover configuration mode to configure sending MPLS trace down all multiple paths (tree trace).</td>
</tr>
<tr>
<td><code>force-explicit-null</code></td>
<td>(Optional) Add an explicit null label to all echo request packets of an IP SLAs Health Monitor operation.</td>
</tr>
<tr>
<td><code>hours-or-statistics kept hours</code></td>
<td>(Optional) Set the number of hours for which LSP discovery group statistics are maintained for an LSP Health Monitor operation.</td>
</tr>
</tbody>
</table>

### Configuring ECMP IP SLAs Tree Trace

Beginning in privileged EXEC mode, follow these steps to use the LSP Health Monitor to configure IP SLAs ECMP tree trace:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td><code>auto ip sla mpls-lsp-monitor operation-number</code></td>
<td>Specify an LSP Health Monitor operation number and enter auto IP SLAs MPLS configuration mode. The operation number range is from 1 to 2147483647.</td>
</tr>
<tr>
<td>3</td>
<td><code>path-discover</code></td>
<td>Enter IP SLAs MPLS LSP monitor path discover configuration mode to configure sending MPLS trace down all multiple paths (tree trace).</td>
</tr>
<tr>
<td>4</td>
<td><code>force-explicit-null</code></td>
<td>(Optional) Add an explicit null label to all echo request packets of an IP SLAs Health Monitor operation.</td>
</tr>
<tr>
<td>5</td>
<td><code>hours-or-statistics kept hours</code></td>
<td>(Optional) Set the number of hours for which LSP discovery group statistics are maintained for an LSP Health Monitor operation.</td>
</tr>
</tbody>
</table>
### Step 6
**Command:** `interval milliseconds`

(Optional) Specify the time interval between MPLS echo requests that are sent as part of the LSP discovery process for an LSP Health Monitor operation.

### Step 7
**Command:** `lsp-selector-base ip-address`

(Optional) Specifies the base IP address used to select the LSPs belonging to the LSP discovery groups of an LSP Health Monitor operation.

### Step 8
**Command:** `maximum-sessions`

(Optional) Set the number of concurrent active tree trace request to be submitted. This is the maximum number of BGP next hop neighbors that can be concurrently undergoing LSP discovery for a single LSP Health Monitor operation.

**Note:** Use careful consideration when configuring this parameter to avoid a negative impact on the switch CPU.

### Step 9
**Command:** `scan-period minutes`

(Optional) Set a time period in minutes for completing tree trace discovery. This is the amount of time after which the LSP discovery process can restart for an LSP Health Monitor operation.

### Step 10
**Command:** `session timeout seconds`

(Optional) Set a timeout value in seconds for tree trace requests. This is the amount of time the LSP discovery process for an LSP Health Monitor operation waits for a response to its LSP discovery request for a particular BGP next hop neighbor.

### Step 11
**Command:** `timeout seconds`

(Optional) Set the amount of time the LSP discovery process for an LSP Health Monitor operation waits for a response to its echo request packets.

**Note:** Use careful consideration when configuring this parameter to avoid a negative impact on the switch CPU.

### Step 12
**Command:** `exit`

Exit IP SLA MPLS LSP monitor path discover configuration mode and return to auto IP SLA MPLS parameter configuration mode.

### Step 13
**Command:** `exit`

Exit auto IP SLA MPLS parameter configuration mode and returns to global configuration mode.
| Step 14 | **auto ip sla mpls-lsp-monitor reaction-configuration operation-number react lpd [lpd-group [retry number] | tree-trace] [action-type trapOnly]** | (Optional) Configure LSP Health Monitor tree trace actions:  
- **operation-number**—Enter the Health Monitor tree-trace operation number.  
- **react lpd**—Specify LPD as the element to be monitored for violations.  
- **lpd-group**—Enable monitoring of LSP discovery group status changes.  
- **retry number**—Specify the number of times the equal-cost multipaths belonging to an LSP discovery group are retested when a failure is detected. The value of the number argument is zero by default.  
- **tree-trace**—Enable monitoring of situations where LSP discovery to a BGP next hop neighbor fails.  
- **action-type trapOnly**—Specify the action to take when the threshold event occurs as **trapOnly** to send an SMNP logging trap. |
| Step 15 | **ip sla monitor logging traps** | (Optional) Enable the generation of SNMP system logging messages specific to IP SLAs trap notifications. |
| Step 16 | **auto ip sla mpls-lsp-monitor schedule operation-number schedule-period seconds [frequency seconds] [start-time [hh:mm:ss] [month day | day month] | pending | now | after hh:mm:ss]** | Schedule the time parameters for the LSP Health Monitor.  
- **operation number**—Enter the IP SLAs MPLS LSP monitor operation number.  
- **schedule-period seconds**—Enter the schedule period in seconds. The range is 1 to 604800 seconds.  
- **frequency seconds**—Enter the frequency for LSP monitoring. The range is 1 to 604800 seconds.  
- **start-time**—Enter the time for the operation to begin collecting information:  
  - To start at a specific time, enter the hour, minute, second and day of the month. If no month is entered, the default is the current month.  
  - Enter **pending** to select no information being collected until a start time is selected.  
  - Enter **now** to start the operation immediately.  
  - Enter **after hh:mm:ss** to indicate that the operation should start after the entered time has elapsed. |
| Step 17 | **end** | Return to privileged EXEC mode. |
| Step 18 | **show ip sla mpls-lsp-monitor configuration [operation-number]** | Show the configured LSP monitoring operations. |
Any Transport over MPLS (AToM) is a solution for transporting Layer 2 packets over an MPLS network, allowing service providers to use the MPLS network to provide connectivity between customer sites with existing Layer 2 networks. Instead of separate networks with network management environments, service providers can use the MPLS network to transport all types of traffic for different customers. The Catalyst 3750 Metro switch supports EoMPLS, a subset of AToM that uses a tunneling mechanism to carry Layer 2 Ethernet traffic.

EoMPLS encapsulates Ethernet frames in MPLS packets and forwards them across the MPLS network. Each frame is sent as a single packet, and the provider-edge (PE) routers connected to the backbone add and remove labels as appropriate for packet encapsulation:

- The ingress PE router receives an Ethernet frame and encapsulates the packet by removing the preamble, the start of frame delimiter (SFD), and the frame check sequence (FCS). The rest of the packet header is not changed.

- The ingress PE router adds a point-to-point virtual connection label and a label switched path (LSP) tunnel label for normal MPLS routing through the MPLS backbone.

- The network core routers use the LSP tunnel label to move the packet through the MPLS backbone and do not distinguish Ethernet traffic from any other types of packets in the MPLS backbone.

- At the other end of the MPLS backbone, the egress PE router receives the packet and de-encapsulates the packet by removing the LSP tunnel label if one is present. The PE router also removes the virtual-connection label from the packet.

- The provider-edge router updates the header, if necessary, and sends the packet out the appropriate interface to the destination switch.

The MPLS backbone uses the tunnel labels to send the packet between the PE routers. The egress PE router uses the virtual-connection label to select the outgoing interface for the Ethernet packet. EoMPLS tunnels are unidirectional; for bidirectional EoMPLS, you need to configure one tunnel in each direction.

The point-to-point virtual connection requires you to configure virtual-connection endpoints at the two PE routers. Only the provider-edge routers at the ingress and egress points of the MPLS backbone are aware of the virtual connections dedicated to transporting Layer 2 traffic. Other routers do not have table entries for these virtual connections.

This section includes additional information about these topics:

- Interaction with Other Features, page 44-41
- EoMPLS Limitations, page 44-42
Interaction with Other Features

This section describes how EoMPLS interacts other features. It includes these sections:

- EoMPLS and IEEE 802.1Q Tunneling, page 44-41
- EoMPLS and Layer 2 Tunneling, page 44-42
- EoMPLS and QoS, page 44-42

EoMPLS and IEEE 802.1Q Tunneling

IEEE 802.1Q tunneling enables service providers to use a single VLAN to support customers who have multiple VLANs, while preserving customer VLAN IDs and segregating traffic in different VLANs. For more information about IEEE 802.1Q tunneling, see Chapter 15, “Configuring IEEE 802.1Q and Layer 2 Protocol Tunneling.”

Figure 44-4 is an example configuration where IEEE 802.1Q-tunneled traffic is forwarded using EoMPLS over an MPLS network. To support IEEE 802.1Q tunneling in a topology where a Layer 2 device connects to an MPLS network through a switch functioning as a provider-edge device, the ingress LAN port on the PE that receives the IEEE 802.1Q tunnel-encapsulated traffic (PE1) is configured as a tunnel port that accepts VLAN 100 traffic. On PE1, the interface is configured for port-based EoMPLS forwarding, with PE2 as the destination IP address. When packets from VLANs 10 to 50 arrive from CE1, they are encapsulated in VLAN 100 and sent to the PE1 egress port that is connected to the MPLS network. At the egress port, an MPLS tag is added to the frame header before it is mapped to a virtual connection and forwarded to the next MPLS PE (PE2).

By entering the `mpls l2transport route` or the `xconnect` interface configuration command on either a VLAN for VLAN-based EoMPLS or an Ethernet port for port-based EoMPLS, you can configure an EoMPLS tunnel to forward traffic based on either the customer VLAN or the Ethernet port.

- To forward IEEE 802.1Q tunnel-encapsulated traffic through the MPLS core to a specific recipient on the other side of the MPLS network, configure port-based EoMPLS.
- To forward IEEE 802.1Q tunnel-encapsulated traffic from an access device to a provider-edge router, configure VLAN-based EoMPLS.
Understanding EoMPLS

EoMPLS and Layer 2 Tunneling

Layer 2 protocol tunneling over an EoMPLS link allows CDP, STP, and VTP protocol data units (PDUs) to be tunneled through an MPLS network. To support Layer 2 protocol tunneling when the Layer 2 device connects to an MPLS network through a switch functioning as a PE, you configure the ingress port on the provider-edge that receives the Layer 2 protocol traffic as a tunnel port. The Layer 2 protocol traffic is encapsulated before it is forwarded over the MPLS network. For more information about Layer 2 protocol tunneling, see Chapter 15, “Configuring IEEE 802.1Q and Layer 2 Protocol Tunneling.”

EoMPLS and QoS

EoMPLS supports QoS by using three experimental bits in a label to determine the priority of packets. To support QoS between label edge routers (LERs), you set the experimental bits in both the virtual connection and the tunnel labels. EoMPLS QoS classification occurs on ingress, and you can only match on Layer 3 parameters (such as IP or DSCP), not Layer 2 parameters (CoS). See the “Configuring MPLS and EoMPLS QoS” section on page 44-51 for more information about EoMPLS and QoS.

EoMPLS Limitations

These restrictions apply to EoMPLS:

- EoMPLS requires that at least one of the two ES ports be configured for MPLS.
- MTU—EoMPLS does not support packet fragmentation and reassembly. Therefore, the maximum transmission unit (MTU) of all intermediate links between endpoints must be sufficient to carry the largest Layer 2 VLAN received. The ingress and egress provider-edge routers must have the same MTU value.
- Address Format—All loopback addresses on provider-edge routers must be configured with 32-bit masks to ensure proper operation of MPLS forwarding. OSPF requires the use of loopback addresses.
- Packet Format—EoMPLS supports VLAN packets that conform to the IEEE 802.1Q standard. ISL encapsulation is not supported between provider-edge and customer-edge routers.
- The maximum number of VLANs using EoMPLS on a switch is 1005.
- Layer 2 connection restrictions:
  - You cannot have a direct Layer 2 connection between provider-edge routers with EoMPLS.
  - You cannot have more than one Layer 2 connection between routers if those routers are configured to transport Ethernet VLANs over the MPLS backbone. Adding a second Layer 2 connection causes the spanning-tree state to constantly toggle if you disable spanning tree on the peer router.
- STP—Do not enable per-VLAN spanning-tree (PVST) on the VLAN configured for an EoMPLS session. STP instances are not supported on this VLAN. All PVST bridge protocol data units (BPDUs) coming in on the EoMPLS VLAN from the customer side are tunneled transparently as data packets over to the EoMPLS pseudowire and vice-versa.
- Trunking—The native VLAN of a trunk cannot be an EoMPLS VLAN.
- You can enable EoMPLS on IEEE 802.1Q interfaces by using the `mpls l2transport route` or the `xconnect` interface configuration command. Use the `xconnect` command if you want to configure pseudowire redundancy.
- Do not configure VLAN mapping on an interface configured for EoMPLS.
Enabling EoMPLS

This section includes this information about configuring EoMPLS on a switch used as a provider-edge router:

- Default EoMPLS Configuration, page 44-43
- EoMPLS Configuration Guidelines, page 44-43
- Configuring EoMPLS, page 44-44
- Packet Flow in an EoMPLS Network, page 44-45
- Configuring L2VPN Pseudowire Redundancy, page 44-46

For more information about EoMPLS commands, see the command reference for this release.

Default EoMPLS Configuration

By default, EoMPLS is not configured.

The `mpls ldp router-id` command is disabled. No virtual connections are configured.

EoMPLS Configuration Guidelines

When you configure EoMPLS, you must follow these guidelines:

- EoMPLS requires that at least one of the two ES ports be configured for MPLS.
- Before enabling EoMPLS, you must enable dynamic MPLS labeling by using the `mpls ip` interface configuration command on all paths between the imposition and disposition LERs. MPLS is globally enabled by default.
- For VLAN-based EoMPLS, you must configure VLANs on the switch.
- EoMPLS operation between two provider-edge routers requires an LDP session between the routers. The IP address used by each router as its LDP router ID must be reachable through IP by the other. Use the optional `mpls ldp router-id` global configuration command to control the selection of the LDP router ID by specifying the interface whose IP address should be used.
  - If the specified interface is up and has an IP address, you can use the command without the optional `force` keyword. When the router ID is selected, that IP address is selected as the router ID.
  - If the specified interface is not up or does not have an IP address, use the `force` keyword with the command to ensure that the IP address of the specified interface is used when that interface is brought up.
- Both provider-edge routers require a loopback address that you can use to create a virtual connection between the routers. When you use OSPF as the interior gateway protocol, you must configure all loopback addresses on provider-edge routers with 32-bit masks to ensure proper operation of MPLS forwarding between the provider-edge routers.
- Do not configure EoMPLS on an interface configured for VLAN mapping.
Enabling EoMPLS

Starting with Cisco IOS Release 12.2(44)SE, when you configure port-based EoMPLS on a Layer 3 interface, you can enter the `mac address-table learning interface interface-id` global configuration command to enable MAC address learning on the port. This ensures that bidirectional traffic can occur at line rate. However, when MAC address learning is enabled, duplicate MAC addresses across VLANs are not supported. An example would be running HSRP groups across the port-based EoMPLS session.

Configuring EoMPLS

You configure VLAN-based EoMPLS on a VLAN interface. When VLAN-based EoMPLS is enabled, the switch associates the tunnel and virtual-connection labels based on the VLAN ID.

Beginning in privileged EXEC mode, follow these steps on the provider-edge routers to configure EoMPLS to transport Layer 2 packets between two endpoints:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 mpls label protocol ldp</td>
<td>Enable LDP for all interfaces. By default, TDP is enabled. This command causes all interfaces to use LDP.</td>
</tr>
<tr>
<td>Step 3 interface loopback0</td>
<td>Enter interface configuration mode for a loopback interface.</td>
</tr>
<tr>
<td>Step 4 ip address ip-address subnet mask</td>
<td>Assign an IP address to the loopback interface.</td>
</tr>
<tr>
<td>Step 5 exit</td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td>Step 6 mpls ldp router-id loopback0 force</td>
<td>(Optional) Force the IP address of loopback interface 0 to be used as the router ID.</td>
</tr>
<tr>
<td>Step 7 mac address-table learning interface interface-id</td>
<td>(Optional) For port-based EoMPLS, enable MAC address learning on the Layer 3 interface.</td>
</tr>
<tr>
<td>Step 8 interface interface-id</td>
<td>Enter a Layer 3 VLAN (for VLAN-based EoMPLS) or the interface ID of a standard port (for port-based EoMPLS), and enter interface configuration mode.</td>
</tr>
</tbody>
</table>
| Step 9 mpls l2transport route destination vc-id or xconnect destination vc-id encapsulation mpls | Configure the interface to transport the Layer 2 VLAN packets over MPLS. 
  • `destination`—IP address of the provider-edge router at the other end of the virtual connection.
  • `vc-id`—Unique value defined for the virtual connection. The VC-ID connects the end points of the virtual connection and must be the same on both ends of the connection. The range is from 1 to 4294967295. |

**Note** Use the `xconnect` command if pseudowire redundancy is required.

| Step 10 end                                  | Return to privileged EXEC mode.                                         |
| Step 11 show mpls l2transport vc             | Verify the configuration.                                               |
| Step 12 copy running-config startup-config   | (Optional) Save your entries in the configuration file.                 |

Use the `no mpls l2transport route destination vc-id` or `no xconnect destination vc-id encapsulation mpls` interface command to delete the EoMPLS tunnel.
This example shows how to configure an EoMPLS tunnel between switch PE1’s VLAN 3 interface and PE2’s VLAN 4 interface.

PE1 has an IP address 10.0.0.1/32, and PE2 has IP address 20.0.01/32. Both provider-edge routers are configured with an MPLS connection to the MPLS core. The VC ID is 123.

Enter these commands on the PE1 switch:

```plaintext
Switch(config)# interface loopback0
Switch(config-if)# ip address 10.10.10.10 255.255.255.255
Switch(config-if)# exit
Switch(config)# interface vlan 3
Switch(config-if)# mpls l2transport route 20.0.0.1 123
```

Enter these commands on the PE2 switch:

```plaintext
Switch(config)# interface loopback0
Switch(config-if)# ip address 20.20.20.20 255.255.255.255
Switch(config-if)# exit
Switch(config)# interface vlan 4
Switch(config-if)# mpls l2transport route 10.0.0.1 123
```

Packet Flow in an EoMPLS Network

Figure 44-5 is an example of packet flow in an EoMPLS network. A customer port on PE1 is configured for a per-port EoMPLS tunnel to a remote customer port on PE2. This allows the two physically separated customer switches (A and B) connected to these ports to appear as if they are directly connected on the same physical LAN.

The EoMPLS tunnel is configured with the IP address of Switch B and a VC ID that is associated with the remote customer port. PE1 establishes a tunnel LSP with PE2 by using a label advertised with LDP by Router A, which is connected to the ES port of PE1. PE1 then establishes a targeted LDP session to PE2 to advertise the virtual-connection label associated with the VC ID. When PE2 is configured with the EoMPLS tunnel, it also establishes a targeted LDP session to advertise the virtual-connection label it associated to the VC ID. This establishes an EoMPLS tunnel between the two ES ports on switch PE1 and switch PE2.

Assume that Host A is connected to the customer switch on VLAN 3 that has a trunk port connected to PE1 configured for IEEE 802.1Q tagging. Host A sends a packet to Host B, using the specific values of MAC addresses, labels, and VLANs shown in the figure. The customer switch tags the host packet and forwards it over the trunk port to PE1.
The tagged packet is received on the customer-edge port that is configured for per-port EoMPLS tunneling. The PE1 switch examines the packet headers and looks at the tables stored in the switch to determine what to do with the packet. Because the port is configured for per-port EoMPLS tunneling, the switch does not remove any VLAN tags that are in the packet, but assigns the packet to an internal VLAN. Only the customer port and the ES port are configured with that internal VLAN, which makes the PE1 ES port the only possible destination for the packet.

The ES port encapsulates the packet header with the tunnel label and the virtual-connection label and forwards the packet to the next hop, in this case Router A, to send it across the MPLS network.

The router receives the packet and forwards it over the MPLS network to the remote PE2 switch. PE2 removes the MPLS encapsulation and sends the packet out the port associated with the virtual-connection label. Customer Switch B removes the final VLAN tag and forwards the packet to the remote host B.

VLAN-based EoMPLS packet flow is basically the same as port-based EoMPLS, except that the customer VLAN is used instead of an internal VLAN. The PE1 switch looks up the customer VLAN ID to determine that the packet is forwarded to the ES port, where the packets is again examined and encapsulated with the tunnel label and virtual-connection label based on the EoMPLS for that VLAN.

Configuring L2VPN Pseudowire Redundancy

Successful transmission of Layer 2 frames between PE routers requires a connection, called a pseudowire, between the routers. You can use the L2VPN pseudowire redundancy feature to configure your network to detect a failure in the network and reroute the Layer 2 service to another endpoint that can continue to provide service. This feature provides the ability to recover from a failure of either the remote provider edge (PE) router or of the link between the PE and customer edge (CE) routers.

For more information see this URL:

L2VPNs also provide pseudowire resiliency through their routing protocols. When connectivity between end-to-end PE routers fails, an alternative path is provided between the directed LDP session and the user data. However, there are some parts of the network where this rerouting mechanism does not protect against interruptions in service. Figure 44-6 shows those parts of the network that are vulnerable to an interruption in service.

**Figure 44-6 Points of Potential Failure in an L2 VPN Network**

X1 = End-to-end routing failure  
X2 = PE hardware or software failure  
X3 = Attachment circuit failure from a line break  
X4 = CE hardware or software failure

L2VPN pseudowire redundancy provides the ability to ensure that the CE2 router in Figure 44-6 can always maintain network connectivity, even if one or all of the failures in the figure occur. You can configure a backup pseudowire so that if the primary pseudowire fails, the provider-edge router switches
to the backup pseudowire. You can configure the primary pseudowire to resume operation after it restarts. You can also configure the network with redundant pseudowires and redundant network elements (routers).

Figure 44-7 shows a network with redundant pseudowires and redundant attachment circuits. You can also optionally configure the network with redundant CE routers and redundant PE routers.

**Figure 44-7  L2 VPN Network with Redundant Pseudowires and Attachment Circuits**

This section includes this information
- Configuration Guidelines, page 44-47
- Configuring the Pseudowire, page 44-48
- Configuring L2VPN Interworking, page 44-48
- Configuring Pseudowire Redundancy, page 44-49
- Forcing a Manual Switchover to the Backup Pseudowire VC, page 44-50
- Monitoring L2VPN Pseudowire Redundancy, page 44-51

**Configuration Guidelines**

Follow these guidelines when configuring L2 VPN pseudowire redundancy:
- The default Label Distribution Protocol (LDP) session hold-down timer enables the software to detect failures in about 180 seconds. You can use the `mpls ldp holdtime` global configuration command to configure the switch to detect failures more quickly.
- The primary and backup pseudowires must run the same type of transport service. You must configure Any Transport over MPLS (AToM) on both the primary and backup pseudowires.
- L2VPN pseudowire redundancy does not support different pseudowire encapsulation types on the MPLS pseudowire.
- L2VPN pseudowire redundancy does support setting the experimental (EXP) bit on the MPLS pseudowire.
- The switch does not support LDP MAC address withdrawal.
- The `mpls l2transport route` command is not supported. Use the `xconnect` command instead.
- The backup pseudowire cannot be operational at the same time that the primary pseudowire is operational. The backup pseudowire becomes active only after the primary pseudowire fails.
- VCCV is supported only on the active pseudowire.
- The switch does not support more than one backup pseudowire.
Enabling EoMPLS

Chapter 44 Configuring MPLS, MPLS VPN, MPLS OAM, and EoMPLS

Configuring the Pseudowire

The pseudowire-class configuration specifies the characteristics of the tunneling mechanism, including encapsulation type and control protocol. You must specify the *encapsulation mpls* command as part of the pseudowire class for the AToM VCs to work properly.

Beginning in privileged EXEC mode, follow these steps to configure a pseudowire class:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td><code>pseudowire-class name</code></td>
<td>Create a pseudowire class with the specified name and enter pseudowire class configuration mode.</td>
</tr>
<tr>
<td>3</td>
<td><code>encapsulation mpls</code></td>
<td>Specify tunneling encapsulation. For AToM, the encapsulation type is <em>mpls</em>.</td>
</tr>
<tr>
<td>4</td>
<td><code>preferred-path interface tunnel tunnel-id</code></td>
<td>(Optional) Specify the path that pseudowire traffic uses to be an MPLS TE tunnel.</td>
</tr>
<tr>
<td>5</td>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>6</td>
<td><code>show mpls l2transport vc [detail]</code></td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td>7</td>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

This example configures the pseudowire class test.

```
Switch# config t
Switch(config)# pseudowire-class test
Switch(config-pw-class)# encapsulation mpls
```

This example shows the output of the `show mpls l2transport vc` command when the primary attachment circuit is up and the backup attachment circuit is available, but not currently selected.

```
Switch# show mpls l2transport vc

<table>
<thead>
<tr>
<th>Local intf</th>
<th>Local circuit</th>
<th>Dest address</th>
<th>VC ID</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>VL120</td>
<td>Eth VLAN 20</td>
<td>10.1.1.2</td>
<td>20</td>
<td>UP</td>
</tr>
<tr>
<td>VL120</td>
<td>Eth VLAN 20</td>
<td>10.1.1.4</td>
<td>20</td>
<td>DOWN</td>
</tr>
</tbody>
</table>
```

Configuring L2VPN Interworking

Layer 2 transport over MPLS and IP exists for like-to-like attachment circuits, such as Ethernet-to-Ethernet. L2VPN interworking builds on this functionality by allowing disparate attachment circuits to be connected. An interworking function facilitates the translation between the different Layer 2 encapsulations.

For information about L2VPN interworking, see the *L2VPN Interworking* feature module at this URL:


Note that the Catalyst 3750 Metro switch does not support ATM interfaces, Point-to-Point Protocol (PPP), or frame relay as mentioned in this document. It also does not support Layer 2 Tunnel Protocol Version 3 (L2TPv3).

L2VPN interworking on the Catalyst 3650 Metro switch works in either Ethernet mode or VLAN mode. You specify the mode by entering the `interworking (ethernet | vlan)` command in pseudowire-class configuration mode. Although visible in the command-line interface help, the *ip* keyword is not supported. Entering the `interworking` command causes the attachment circuits to be terminated locally.
The keywords perform these functions:

- The `ethernet` keyword causes Ethernet frames to be extracted from the attachment circuit and sent over the pseudowire. Ethernet end-to-end transmission is assumed. Attachment circuit frames that are not Ethernet are dropped.

- The `vlan` keyword causes VLAN-tagged packets to be extracted and sent over the pseudowire. Frames that are not VLAN-tagged are dropped.

Beginning in privileged EXEC mode, follow these steps to configure L2VPN VLAN interworking on a PE router:

```
Step 1 configure terminal Enter global configuration mode.
Step 2 pseudowire-class name Create a pseudowire class with the specified name and enter pseudowire class configuration mode.
Step 3 encapsulation mpls Specify tunneling encapsulation. For AToM, the encapsulation type is `mpls`.
Step 4 interworking {ethernet | vlan} Enable interworking and specify the translation method.
  • `ethernet`—Send Ethernet packets across the pseudowire.
  • `vlan`—Send VLAN-tagged packets across the pseudowire.
  
  **Note** Although visible in the CLI, the `ip` keyword is not supported.

Step 5 end Return to privileged EXEC mode.
Step 6 show mpls l2transport vc [detail] Verify the configuration.
Step 7 copy running-config startup-config (Optional) Save your entries in the configuration file.
```

This example shows how to configure VLAN interworking:

```
Switch# configure terminal
Switch(config)# pseudowire-class test
Switch(config-pw-class)# encapsulation mpls
Switch(config-pw-class)# interworking vlan
Switch(config-pw-class)# exit
```

For a more detailed configuration example, see the configuration example for “Ethernet to VLAN over AToM (Bridged): Example” in the L2VPN Interworking feature module.

### Configuring Pseudowire Redundancy

When configuring pseudowire redundancy, you use the `xconnect` interface configuration command for each transport type. Beginning in privileged EXEC mode, follow these steps to configure pseudowire redundancy on a PE router:

```
Step 1 configure terminal Enter global configuration mode.
Step 2 interface interface-id Specify an interface and enter interface configuration mode. The interface on the adjoining router must be on the same VLAN as this router.
```
Enabling EoMPLS

Step 3  
```
xconnect peer-router-id vcid encapsulation mpls
  pw-class pw-class name
```
Bind the attachment circuit to a pseudowire virtual circuit (VC) and enter `xconnect` configuration mode.

*Note*  You must specify MPLS encapsulation. If you omit the `encapsulation mpls` command as part of the `xconnect` command, you receive an `Incomplete command` error message.

Step 4  
```
backup peer peer-router-ip-address vcid [pw-class pw-class name]
```
Specify a redundant peer for the pseudowire VC. If you do not specify a `pw-class name`, the value is inherited from the parent.

Step 5  
```
backup delay enable-delay {disable-delay | never}
```
Specify the delays before pseudowire takeovers.

- `enable-delay`— Specify how long (in seconds) the backup pseudowire VC waits to take over after the primary pseudowire VC goes down. The range is 0 to 180 seconds; the default is 0.

- `disable-delay`— Specify how long (in seconds) the primary pseudowire waits after it becomes active to take over from the backup pseudowire. The range is 0 to 180 seconds; the default is 0.

- If you enter `never`, the switchback to the primary pseudowire never occurs.

Step 6  
```
end
```
Return to privileged EXEC mode.

Step 7  
```
show xconnect all
```
Verify the configuration.

Step 8  
```
copy running-config startup-config
```
(Optional) Save your entries in the configuration file.

This example shows how to configure pseudowire redundancy as a switchover to the peer with the IP address 10.1.1.12 immediately when a failure occurs and to not switch back to the primary VC when it becomes available.

```
Switch# config t
Switch(config)# interface gigabitethernet1/1/1
Switch (config-if)# xconnect 10.1.1.4 33 encapsulation mpls
Switch(config-if-xconn)# backup peer 10.1.1.2 33
Switch(config-if-xconn)# backup delay 0 never
```

Forcing a Manual Switchover to the Backup Pseudowire VC

You can manually force the router to switch to the backup or primary pseudowire. You can specify either the interface of the primary attachment circuit or the IP address and VC ID of the peer router. If the specified interface or peer is not available, the switchover does not occur. The backup pseudowire becomes active when you enter the command.

Beginning in privileged EXEC mode, follow these steps to force a pseudowire switchover:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1  
```
xconnect backup force-switchover {interface interface-id | peer ip-address voiced}
```
Specify that the router should switch to the backup or to the primary pseudowire when the command is entered.
This command forces a switchover to the peer with the IP address 10.1.1.4 and VCID 33.

```
Switch# xconnect backup force-switchover peer 10.1.1.4 33
```

### Monitoring L2VPN Pseudowire Redundancy

Use the privileged EXEC commands in Table 44-2 to verify or monitor pseudowire redundancy.

#### Table 44-1 Commands for Displaying MPLS and EoMPLS Information

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show xconnect {all</td>
<td>interface</td>
</tr>
<tr>
<td>show mpls l2transport vc [detail] [summary]</td>
<td>Display detailed or summary information about the active virtual connections that are enabled to route Layer 2 packets on a provider-edge device.</td>
</tr>
</tbody>
</table>

You can also use the `xconnect logging redundancy` global configuration command to track the status of the xconnect redundancy group. The command generates messages during switchover events.

### Configuring MPLS and EoMPLS QoS

Quality of service (QoS) in MPLS and EoMPLS enables network administrators to provide differentiated types of service across an MPLS network. Each packet can receive the particular kind of service specified by the packet QoS. To preserve QoS IP precedence bits, you must globally disable QoS.

After you enable QoS, you can preserve Differentiated Services Code Point (DSCP) or IP precedence bits by using a trusted configuration at the interface level. For more information, see the “Configuring Ingress Classification by Using Port Trust States” section on page 34-56. However, the unpreserved bits are automatically overwritten by the value of the preserved bits. For example, if you preserve the DSCP bits, the IP precedence and CoS bits are overwritten with the value of the DSCP bits. You can also set MPLS and EoMPLS QoS priority by using 3 experimental bits in the MPLS label to determine the priority of packets.

**Note**

The switch supports only DSCP and IP precedence classification for MPLS and EoMPLS.

This section contains this information:

- Understanding MPLS QoS, page 44-51
- Enabling MPLS and EoMPLS QoS, page 44-53

### Understanding MPLS QoS

Service in an MPLS network can be specified in different ways, for example, by using the IP precedence bit settings in IP packets. When you send IP packets from one site to another, the IP precedence field (the first 3 bits of the DSCP field in the header of an IP packet) specifies the QoS. Based on the IP precedence marking, the packet is given the desired treatment such as latency or bandwidth. If the network is an MPLS network, the IP precedence bits are copied into the MPLS EXP field at the edge of the network.
A service provider might also want to set a QoS value for an MPLS packet to a different value. Instead of overwriting the value in the IP precedence field that belongs to a customer, the service provider can set the MPLS experimental field. The IP header remains available for the customer’s use, and the QoS of an IP packet is not changed as the packet travels through the MPLS network.

By choosing different values for the MPLS experimental field, you can mark packets based on their characteristics, such as rate or type, so that packets have the priority that they require during periods of congestion.

Figure 44-8 shows an MPLS network that connects two sites of an IP network that belongs to a customer.

**Figure 44-8**  **MPLS Network Connecting Two Customer Sites**

PE1 and PE2 are customer-located routers at the boundaries between the MPLS network and the IP network and are the ingress and egress provider-edge devices. CE1 and CE2 are customer edge devices. P1 and P2 are service provider routers within the core of the service-provider network.

Packets arrive as IP packets at PE1, the ingress provider-edge router, and PE1 sends the packets to the MPLS network as MPLS packets. Within the service-provider network, there is no IP precedence field for the queuing mechanism to look at because the packets are MPLS packets. The packets remain as MPLS packets until they arrive at PE2, the egress provider-edge router. PE2 removes the label from each packet and forwards the packets as IP packets.

MPLS QoS enables service providers to classify packets according to their type, input interface, and other factors by setting (marking) each packet within the MPLS experimental field without changing the IP precedence or DSCP field. You can use the IP Precedence or DSCP bits to specify the QoS for an IP packet and use the MPLS experimental bits to specify the QoS for an MPLS packet. In an MPLS network, configure the MPLS experimental field value at PE1 (the ingress router) to set the QoS value in the MPLS packet.

It is important to assign the correct priority to a packet. The priority of a packet affects how the packet is treated during periods of congestion. For example, service providers have service-level agreements with customers that specify how much traffic the service provider has agreed to deliver. To comply with the agreement, the customer must not send more than the agreed-upon rate. Packets are considered to be in-rate or out-of-rate. If there is congestion in the network, out-of-rate packets might be dropped more aggressively.
Enabling MPLS and EoMPLS QoS

This section describes how to configure MPLS QoS on the ingress provider-edge router. It includes these topics:

- Default MPLS and EoMPLS QoS Configuration, page 44-53
- Setting the Priority of Packets with Experimental Bits, page 44-53
- Configuring MPLS VPN QoS, page 44-55

For more information about QoS, see Chapter 34, “Configuring QoS.”

Default MPLS and EoMPLS QoS Configuration

QoS is disabled. Packets are not modified, and the CoS, DSCP, and IP precedence values in the packet are not changed. Traffic is switched in pass-through mode (packets are switched without any rewrites and classified as best effort without any policing).

The default behavior for the VLAN-based EoMPLS packets is to relay the IEEE 802.1p bits into the EXP bits of the virtual-connection and tunnel labels. The default behavior for the port-based EoMPLS packets is to use a value of 0 in the EXP bits of the virtual-connection and tunnel labels. You can change the default behavior for VLAN- or port-based EoMPLS by applying a hierarchical QoS policy on an ES port.

When QoS is enabled with the `mls qos` global configuration command and all other QoS settings are at their defaults, traffic is classified as best effort (the DSCP value is set to 0) without any policing. No policy maps are configured.

---

Note

For MPLS and EoMPLS QoS, you can match only Layer 3 parameters (IP or DCSP values), not Layer 2 (CoS values).

Setting the Priority of Packets with Experimental Bits

MPLS and EoMPLS provide QoS on the ingress router by using 3 experimental bits in a label to determine the priority of packets. To support QoS between LERs, set the experimental bits in both the virtual-connection and tunnel labels. If you do not assign values to the experimental bits, the priority bits in the IEEE 802.1Q header tag control information field are written into the experimental bit fields.

The process includes these steps on the ingress router:

- Configure a class map to classify IP packets according to their DSCP or IP precedence classification.

  Note

  The switch supports only DSCP and IP precedence classification for MPLS and EoMPLS.

- Configure a policy map to mark MPLS packets (write their classification into the MPLS experimental field).

- Configure the input interface to attach the service policy.
Beginning in privileged EXEC mode, follow these steps to set the experimental bits for EoMPLS or MPLS QoS:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>mls qos</td>
</tr>
<tr>
<td>Step 3</td>
<td>class-map class-map-name</td>
</tr>
<tr>
<td>Step 4</td>
<td>match {ip dscp dscp-list</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>The switch does not support the cos and vlan keywords for MPLS and EoMPLS.</td>
</tr>
<tr>
<td>Step 5</td>
<td>exit</td>
</tr>
<tr>
<td>Step 6</td>
<td>policy-map policy-map-name</td>
</tr>
<tr>
<td>Step 7</td>
<td>class class-name</td>
</tr>
<tr>
<td>Step 8</td>
<td>set mpls experimental exp-number</td>
</tr>
<tr>
<td>Step 9</td>
<td>exit</td>
</tr>
<tr>
<td>Step 10</td>
<td>exit</td>
</tr>
<tr>
<td>Step 11</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 12</td>
<td>service-policy output policy-map-name</td>
</tr>
<tr>
<td>Step 13</td>
<td>end</td>
</tr>
<tr>
<td>Step 14</td>
<td>show policy-map [policy-map-name [class class-map-name]] show policy-map interface interface-id</td>
</tr>
<tr>
<td>Step 15</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To delete an existing policy map, use the no policy-map policy-map-name global configuration command. To delete an existing class, use the no class class-name policy-map configuration command.

This example shows how to use class and policy maps to configure different experimental bit settings for DSCP and IP precedence for MPLS QoS.

```
Switch(config)# class-map match-all gold-class
Switch(config-cmap)# match ip dscp 1
Switch(config-cmap)# exit
Switch(config)# class-map match-all silver-class
Switch(config-cmap)# match ip precedence 2
Switch(config-cmap)# exit
```
Switch(config)# policy-map out-policy
Switch(config-pmap)# class gold-class
Switch(config-pmap-c)# set mpls experimental 5
Switch(config-pmap-c)# exit
Switch(config-pmap)# class silver-class
Switch(config-pmap-c)# set mpls experimental 4
Switch(config-pmap-c)# exit
Switch(config)# interface gigabitethernet1/1/1
Switch(config-if)# service-policy output out-policy
Switch(config-if)# end

Configuring MPLS VPN QoS

To perform per VRF QoS, you typically configure the PE router to perform per-VRF QoS functions at the CE-facing interfaces. On the Catalyst 3750 Metro switch, you can apply policers at the SVI and perform per-VRF QoS. However, you can only apply policers on ingress at the SVI; the switch does not support egress policers at the SVI. For more information about hierarchical-QoS policers applied at the SVI, see the “Hierarchical Dual-Level Policing on SVIs” section on page 34-15.

You can apply standard QoS functions to MPLS VPN traffic. However, for a hierarchical QoS function, you cannot apply a service policy that would match traffic on a per VRF basis because VRFs are dynamically assigned to an MPLS label. For MPLS VPN traffic, you can apply a service-policy on egress that matches traffic based on DSCP or MPLS.

Monitoring and Maintaining MPLS and EoMPLS

To clear MPLS counters or display MPLS and EoMPLS information, use the privileged EXEC commands in Table 44-2.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear mpls counters</td>
<td>Clear MPLS forwarding counters.</td>
</tr>
<tr>
<td>clear mpls traffic-eng autotunnel primary</td>
<td>Remove all primary auto tunnels and recreate them.</td>
</tr>
<tr>
<td>show interface tunnel tunnel-number</td>
<td>Display information about the specified tunnel interface.</td>
</tr>
<tr>
<td>show ip explicit paths</td>
<td>Display the configured IP explicit paths.</td>
</tr>
<tr>
<td>show ip rsvp fast reroute [detail]</td>
<td>Display specific information for RSVP categories, including fast reroute.</td>
</tr>
<tr>
<td>show ip rsvp host</td>
<td>Display RSVP terminal point information for receivers or senders</td>
</tr>
<tr>
<td>show isis database verbose</td>
<td>Display information about the IS-IS database.</td>
</tr>
<tr>
<td>show isis mpls traffic-eng</td>
<td>Display information about IS-IS MPLS traffic engineering.</td>
</tr>
<tr>
<td>show mpls forwarding-table</td>
<td>Display the contents of the MPLS label forwarding information base (LFIB).</td>
</tr>
<tr>
<td>show mpls interfaces</td>
<td>Display information about interfaces that have been configured for label switching.</td>
</tr>
<tr>
<td>show mpls ip binding</td>
<td>Display specified information about label bindings learned by LDP.</td>
</tr>
</tbody>
</table>
### Table 44-2 Commands for Displaying MPLS and EoMPLS Information (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show mpls l2transport vc [detail] [summary]</code></td>
<td>Display detailed or summary information about the EoMPLS virtual connections that have been enabled to route Layer 2 packets on a provider-edge device.</td>
</tr>
<tr>
<td><code>show mpls l2transport vc [vc-id] [vc-id-min - vc-id-max]</code></td>
<td>Display information about the specified virtual connection or range of virtual-connections. The range is from 1 to 4294967295.</td>
</tr>
<tr>
<td><code>show mpls label range</code></td>
<td>Display the range of local labels available for use on packet interfaces.</td>
</tr>
<tr>
<td><code>show mpls ldp backoff</code></td>
<td>Display information about the configured session setup backoff parameters and any potential LDP peers with which session setup attempts are being throttled.</td>
</tr>
<tr>
<td><code>show mpls ldp bindings</code></td>
<td>Display the contents of the label information base (LIB).</td>
</tr>
<tr>
<td><code>show mpls ldp discovery</code></td>
<td>Display the status of the LDP discovery process.</td>
</tr>
<tr>
<td><code>show mpls ldp neighbor</code></td>
<td>Display the status of LDP sessions.</td>
</tr>
<tr>
<td><code>show mpls ldp parameters</code></td>
<td>Display current LDP parameters.</td>
</tr>
<tr>
<td><code>show mpls prefix-map</code></td>
<td>Show the prefix map used to assign a QoS map to network prefixes that match a standard IP access list.</td>
</tr>
<tr>
<td><code>show mpls traffic-eng autoroute</code></td>
<td>Display tunnels announced to the IGP, including interface, destination, and bandwidth.</td>
</tr>
<tr>
<td><code>show mpls traffic-eng fast-reroute database</code></td>
<td>Display the contents of the Fast Reroute (FRR) database.</td>
</tr>
<tr>
<td><code>show mpls traffic-eng link-management</code></td>
<td>Display link information about MPLS traffic engineering link management.</td>
</tr>
<tr>
<td><code>show mpls traffic-eng topology</code></td>
<td>Display the MPLS traffic engineering global topology as currently known at a node.</td>
</tr>
<tr>
<td><code>show mpls traffic-eng tunnel</code></td>
<td>Display information about MPLS traffic-engineering tunnels.</td>
</tr>
</tbody>
</table>
This chapter describes how to configure IP multicast routing on the Catalyst 3750 Metro switch. IP multicasting is a more efficient way to use network resources, especially for bandwidth-intensive services such as audio and video. IP multicast routing enables a host (source) to send packets to a group of hosts (receivers) anywhere within the IP network by using a special form of IP address called the IP multicast group address. The sending host inserts the multicast group address into the IP destination address field of the packet, and IP multicast routers and multilayer switches forward incoming IP multicast packets out all interfaces that lead to members of the multicast group. Any host, regardless of whether it is a member of a group, can send to a group. However, only the members of a group receive the message.

Note

For complete syntax and usage information for the commands used in this chapter, see the Cisco IOS IP Command Reference, Volume 3 of 3: Multicast, Release 12.2.

This chapter consists of these sections:
- Understanding Cisco’s Implementation of IP Multicast Routing, page 45-1
- Configuring IP Multicast Routing, page 45-9
- Configuring Advanced PIM Features, page 45-34
- Configuring Optional IGMP Features, page 45-38
- Configuring Optional Multicast Routing Features, page 45-43
- Configuring Basic DVMRP Interoperability Features, page 45-48
- Configuring Advanced DVMRP Interoperability Features, page 45-53
- Monitoring and Maintaining IP Multicast Routing, page 45-61

For information on configuring the Multicast Source Discovery Protocol (MSDP), see Chapter 46, “Configuring MSDP.”

Understanding Cisco’s Implementation of IP Multicast Routing

The Cisco IOS software supports these protocols to implement IP multicast routing:
- Internet Group Management Protocol (IGMP) is used among hosts on a LAN and the routers (and multilayer switches) on that LAN to track the multicast groups of which hosts are members.
- Protocol-Independent Multicast (PIM) protocol is used among routers and multilayer switches to track which multicast packets to forward to each other and to their directly connected LANs.
• Distance Vector Multicast Routing Protocol (DVMRP) is used on the multicast backbone of the Internet (MBONE). The software supports PIM-to-DVMRP interaction.
• Cisco Group Management Protocol (CGMP) is used on Cisco routers and multilayer switches connected to Layer 2 Catalyst switches to perform tasks similar to those performed by IGMP. Figure 45-1 shows where these protocols operate within the IP multicast environment.

Figure 45-1 IP Multicast Routing Protocols

According to IPv4 multicast standards, the MAC destination multicast address begins with 0100:5e and is appended by the last 23 bits of the IP address. On the Catalyst 3750 Metro switch, if the multicast packet does not match the switch multicast address, the packets are treated in this way:

• If the packet has a multicast IP address and a unicast MAC address, the packet is forwarded in software. This can occur because some protocols on legacy devices use unicast MAC addresses with multicast IP addresses.
• If the packet has a multicast IP address and an unmatched multicast MAC address, the packet is dropped.

This section includes this information:
• Understanding IGMP, page 45-2
• Understanding PIM, page 45-3
• Understanding DVMRP, page 45-8
• Understanding CGMP, page 45-9

Understanding IGMP

To participate in IP multicasting, multicast hosts, routers, and multilayer switches must have the IGMP operating. This protocol defines the querier and host roles:

• A querier is a network device that sends query messages to discover which network devices are members of a given multicast group.
• A host is a receiver that sends report messages (in response to query messages) to inform a querier of a host membership.
A set of queriers and hosts that receive multicast data streams from the same source is called a multicast group. Queriers and hosts use IGMP messages to join and leave multicast groups.

Any host, regardless of whether it is a member of a group, can send to a group. However, only the members of a group receive the message. Membership in a multicast group is dynamic; hosts can join and leave at any time. There is no restriction on the location or number of members in a multicast group. A host can be a member of more than one multicast group at a time. How active a multicast group is and what members it has can vary from group to group and from time to time. A multicast group can be active for a long time, or it can be very short-lived. Membership in a group can constantly change. A group that has members can have no activity.

IP multicast traffic uses group addresses, which are class D addresses. The high-order bits of a Class D address are 1110. Therefore, host group addresses can be in the range 224.0.0.0 through 239.255.255.255. Multicast addresses in the range 224.0.0.0 to 24.0.0.255 are reserved for use by routing protocols and other network control traffic. The address 224.0.0.0 is guaranteed not to be assigned to any group.

IGMP packets are sent using these IP multicast group addresses:
- IGMP general queries are destined to the address 224.0.0.1 (all systems on a subnet).
- IGMP group-specific queries are destined to the group IP address for which the switch is querying.
- IGMP group membership reports are destined to the group IP address for which the switch is reporting.
- IGMP Version 2 (IGMPv2) leave messages are destined to the address 224.0.0.2 (all-multicast-routers on a subnet). In some old host IP stacks, leave messages might be destined to the group IP address rather than to the all-routers address.

**IGMP Version 1**

IGMP Version 1 (IGMPv1) primarily uses a query-response model that enables the multicast router and multilayer switch to find which multicast groups are active (have one or more hosts interested in a multicast group) on the local subnet. IGMPv1 has other processes that enable a host to join and leave a multicast group. For more information, see RFC 1112.

**IGMP Version 2**

IGMPv2 extends IGMP functionality by providing such features as the IGMP leave process to reduce leave latency, group-specific queries, and an explicit maximum query response time. IGMPv2 also adds the capability for routers to elect the IGMP querier without depending on the multicast protocol to perform this task. For more information, see RFC 2236.

**Understanding PIM**

PIM is called protocol-independent: regardless of the unicast routing protocols used to populate the unicast routing table, PIM uses this information to perform multicast forwarding instead of maintaining a separate multicast routing table.

PIM is defined in RFC 2362, Protocol-Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification. PIM is defined in these Internet Engineering Task Force (IETF) Internet drafts:
- Protocol Independent Multicast (PIM): Motivation and Architecture
- Protocol Independent Multicast (PIM), Dense Mode Protocol Specification
Understanding Cisco’s Implementation of IP Multicast Routing

This section includes this information about PIM:

- PIM Versions, page 45-4
- PIM Modes, page 45-4
- PIM Stub Routing, page 45-5
- IGMP Helper, page 45-6
- Auto-RP, page 45-6
- Bootstrap Router, page 45-7
- Multicast Forwarding and Reverse Path Check, page 45-7

### PIM Versions

PIMv2 includes these improvements over PIMv1:

- A single, active rendezvous point (RP) exists per multicast group, with multiple backup RPs. This single RP compares to multiple active RPs for the same group in PIMv1.
- A bootstrap router (BSR) provides a fault-tolerant, automated RP discovery and distribution mechanism that enables routers and multilayer switches to dynamically learn the group-to-RP mappings.
- Sparse mode and dense mode are properties of a group, as opposed to an interface. We strongly recommend sparse-dense mode, as opposed to either sparse mode or dense mode only.
- PIM join and prune messages have more flexible encoding for multiple address families.
- A more flexible hello packet format replaces the query packet to encode current and future capability options.
- Register messages to an RP specify whether they are sent by a border router or a designated router.
- PIM packets are no longer inside IGMP packets; they are standalone packets.

### PIM Modes

PIM can operate in dense mode (DM), sparse mode (SM), or in sparse-dense mode (PIM DM-SM), which handles both sparse groups and dense groups at the same time.

### PIM DM

PIM DM builds source-based multicast distribution trees. In dense mode, a PIM DM router or multilayer switch assumes that all other routers or multilayer switches forward multicast packets for a group. If a PIM DM device receives a multicast packet and has no directly connected members or PIM neighbors present, a prune message is sent back to the source to stop unwanted multicast traffic. Subsequent multicast packets are not flooded to this router or switch on this pruned branch because branches without receivers are pruned from the distribution tree, leaving only branches that contain receivers.
When a new receiver on a previously pruned branch of the tree joins a multicast group, the PIM DM device detects the new receiver and immediately sends a graft message up the distribution tree toward the source. When the upstream PIM DM device receives the graft message, it immediately puts the interface on which the graft was received into the forwarding state so that the multicast traffic begins flowing to the receiver.

**PIM SM**

PIM SM uses shared trees and shortest-path-trees (SPTs) to distribute multicast traffic to multicast receivers in the network. In PIM SM, a router or multilayer switch assumes that other routers or switches do not forward multicast packets for a group, unless there is an explicit request for the traffic (join message). When a host joins a multicast group using IGMP, its directly connected PIM SM device sends PIM join messages toward the root, also known as the RP. This join message travels router-by-router toward the root, constructing a branch of the shared tree as it goes.

The RP keeps track of multicast receivers. It also registers sources through register messages received from the source’s first-hop router (designated router [DR]) to complete the shared tree path from the source to the receiver. When using a shared tree, sources must send their traffic to the RP so that the traffic reaches all receivers.

Prune messages are sent up the distribution tree to prune multicast group traffic. This action permits branches of the shared tree or SPT that were created with explicit join messages to be torn down when they are no longer needed.

**PIM Stub Routing**

The PIM stub routing feature reduces resource usage by moving routed traffic closer to the end user.

In a network using PIM stub routing, the only allowable route for IP traffic to the user is through a switch that is configured with PIM stub routing. PIM passive interfaces are connected to Layer 2 access domains, such as VLANs, or to interfaces that are connected to other Layer 2 devices. Only directly connected multicast (IGMP) receivers and sources are allowed in the Layer 2 access domains. The PIM passive interfaces do not send or process any received PIM control packets.

When using PIM stub routing, you should configure the distribution and remote routers to use IP multicast routing and configure only the switch as a PIM stub router. The switch does not route transit traffic between distribution routers. You also need to configure a routed uplink port on the switch. The switch uplink port cannot be used with SVIs. If you need PIM for an SVI uplink port, you should upgrade to the IP services feature set.

You must also configure EIGRP stub routing when configuring PIM stub routing on the switch. For more information, see the “Configuring EIGRP Stub Routing” section on page 36-41.

The redundant PIM stub router topology is not supported. The redundant topology exists when there is more than one PIM router forwarding multicast traffic to a single access domain. PIM messages are blocked, and the PIM assert and designated router election mechanisms are not supported on the PIM passive interfaces. Only the nonredundant access router topology is supported by the PIM stub feature. By using a nonredundant topology, the PIM passive interface assumes that it is the only interface and designated router on that access domain.

In Figure 45-2, Switch A routed uplink port 25 is connected to the router and PIM stub routing is enabled on the VLAN 100 interfaces and on Host 3. This configuration allows the directly connected hosts to receive traffic from multicast source 200.1.1.3. See the “Configuring PIM Stub Routing” section on page 45-13 for more information.
Understanding Cisco’s Implementation of IP Multicast Routing

**Figure 45-2**  PIM Stub Router Configuration

![Diagram of PIM Stub Router Configuration]

**IGMP Helper**

PIM stub routing moves routed traffic closer to the end user and reduces network traffic. You can also reduce traffic by configuring a stub router (switch) with the IGMP helper feature.

You can configure a stub router (switch) with the `igmp helper help-address` interface configuration command to enable the switch to send reports to the next-hop interface. Hosts that are not directly connected to a downstream router can then join a multicast group sourced from an upstream network. The IGMP packets from a host wanting to join a multicast stream are forwarded upstream to the next-hop device when this feature is configured. When the upstream central router receives the helper IGMP reports or leaves, it adds or removes the interfaces from its outgoing interface list for that group.

For complete syntax and usage information for the `ip igmp helper-address` command, see the *Cisco IP Multicast Command Reference*:


**Auto-RP**

This proprietary feature eliminates the need to manually configure the RP information in every router and multilayer switch in the network. For Auto-RP to work, you configure a Cisco router or multilayer switch as the mapping agent. It uses IP multicast to learn which routers or switches in the network are possible candidate RPs to receive candidate RP announcements. Candidate RPs periodically send multicast RP-announce messages to a particular group or group range to announce their availability.

Mapping agents listen to these candidate RP announcements and use the information to create entries in their Group-to-RP mapping caches. Only one mapping cache entry is created for any Group-to-RP range received, even if multiple candidate RPs are sending RP announcements for the same range. As the RP-announce messages arrive, the mapping agent selects the router or switch with the highest IP address as the active RP and stores this RP address in the Group-to-RP mapping cache.

Mapping agents periodically multicast the contents of their Group-to-RP mapping cache. Thus, all routers and switches automatically discover which RP to use for the groups they support. If a router or switch fails to receive RP-discovery messages and the Group-to-RP mapping information expires, it switches to a statically configured RP that was defined with the `ip pim rp-address` global configuration command. If no statically configured RP exists, the router or switch changes the group to dense-mode operation.

Multiple RPs serve different group ranges or serve as hot backups of each other.
Bootstrap Router

PIMv2 BSR is another method to distribute group-to-RP mapping information to all PIM routers and multilayer switches in the network. It eliminates the need to manually configure RP information in every router and switch in the network. However, instead of using IP multicast to distribute group-to-RP mapping information, BSR uses hop-by-hop flooding of special BSR messages to distribute the mapping information.

The BSR is elected from a set of candidate routers and switches in the domain that have been configured to function as BSRs. The election mechanism is similar to the root-bridge election mechanism used in bridged LANs. The BSR election is based on the BSR priority of the device contained in the BSR messages that are sent hop-by-hop through the network. Each BSR device examines the message and forwards out all interfaces only the message that has either a higher BSR priority than its BSR priority or the same BSR priority, but with a higher BSR IP address. Using this method, the BSR is elected.

The elected BSR sends BSR messages with a TTL of 1. Neighboring PIMv2 routers or multilayer switches receive the BSR message and multicast it out all other interfaces (except the one on which it was received) with a TTL of 1. In this way, BSR messages travel hop-by-hop throughout the PIM domain. Because BSR messages contain the IP address of the current BSR, the flooding mechanism enables candidate RPs to automatically learn which device is the elected BSR.

Candidate RPs send candidate RP advertisements showing the group range for which they are responsible to the BSR, which stores this information in its local candidate-RP cache. The BSR periodically advertises the contents of this cache in BSR messages to all other PIM devices in the domain. These messages travel hop-by-hop through the network to all routers and switches, which store the RP information in the BSR message in their local RP cache. The routers and switches select the same RP for a given group because they all use a common RP hashing algorithm.

Multicast Forwarding and Reverse Path Check

With unicast routing, routers and multilayer switches forward traffic through the network along a single path from the source to the destination host whose IP address appears in the destination address field of the IP packet. Each router and switch along the way makes a unicast forwarding decision, using the destination IP address in the packet, by looking up the destination address in the unicast routing table and forwarding the packet through the specified interface to the next hop toward the destination.

With multicasting, the source is sending traffic to an arbitrary group of hosts represented by a multicast group address in the destination address field of the IP packet. To decide whether to forward or drop an incoming multicast packet, the router or multilayer switch uses a reverse path forwarding (RPF) check on the packet as follows and shown in Figure 45-3:

1. The router or multilayer switch examines the source address of the arriving multicast packet to decide whether the packet arrived on an interface that is on the reverse path back to the source.
2. If the packet arrives on the interface leading back to the source, the RPF check is successful and the packet is forwarded to all interfaces in the outgoing interface list (which might not be all interfaces on the router).
3. If the RPF check fails, the packet is discarded.

Some multicast routing protocols, such as DVMRP, maintain a separate multicast routing table and use it for the RPF check. However, PIM uses the unicast routing table to perform the RPF check.

Figure 45-3 shows port 0/2 receiving a multicast packet from source 151.10.3.21. Table 45-1 shows that the port on the reverse path to the source is port 0/1, not port 0/2. Because the RPF check fails, the multilayer switch discards the packet. Another multicast packet from source 151.10.3.21 is received on port 0/1, and the routing table shows this port is on the reverse path to the source. Because the RPF check passes, the switch forwards the packet to all ports in the outgoing port list.
Understanding Cisco’s Implementation of IP Multicast Routing

PIM uses both source trees and RP-rooted shared trees to forward datagrams (described in the “PIM DM” section on page 45-4 and the “PIM SM” section on page 45-5). The RPF check is performed differently for each:

- If a PIM router or multilayer switch has a source-tree state (that is, an (S,G) entry is present in the multicast routing table), it performs the RPF check against the IP address of the source of the multicast packet.

- If a PIM router or multilayer switch has a shared-tree state (and no explicit source-tree state), it performs the RPF check on the RP address (which is known when members join the group).

Sparse-mode PIM uses the RPF lookup function to decide where it needs to send joins and prunes:

- (S,G) joins (which are source-tree states) are sent toward the source.

- (*,G) joins (which are shared-tree states) are sent toward the RP.

DVMRP and dense-mode PIM use only source trees and use RPF as previously described.

Understanding DVMRP

DVMRP is implemented in the equipment of many vendors and is based on the public-domain mrouted program. This protocol has been deployed in the MBONE and in other intradomain multicast networks. Cisco routers and multilayer switches run PIM and can forward multicast packets to and receive from a DVMRP neighbor. It is also possible to propagate DVMRP routes into and through a PIM cloud. The software propagates DVMRP routes and builds a separate database for these routes on each router and multilayer switch, but PIM uses this routing information to make the packet-forwarding decision. The software does not implement the complete DVMRP. However, it supports dynamic discovery of DVMRP routers and can interoperate with them over traditional media (such as Ethernet and FDDI) or over DVMRP-specific tunnels.
DVMRP neighbors build a route table by periodically exchanging source network routing information in route-report messages. The routing information stored in the DVMRP routing table is separate from the unicast routing table and is used to build a source distribution tree and to perform multicast forward using RPF.

DVMRP is a dense-mode protocol and builds a parent-child database using a constrained multicast model to build a forwarding tree rooted at the source of the multicast packets. Multicast packets are initially flooded down this source tree. If redundant paths are on the source tree, packets are not forwarded along those paths. Forwarding occurs until prune messages are received on those parent-child links, which further constrain the broadcast of multicast packets.

**Understanding CGMP**

This software release provides CGMP-server support on your switch; no client-side functionality is provided. The switch serves as a CGMP server for devices that do not support IGMP snooping but have CGMP-client functionality.

CGMP is a protocol used on Cisco routers and multilayer switches connected to Layer 2 Catalyst switches to perform tasks similar to those performed by IGMP. CGMP permits Layer 2 group membership information to be communicated from the CGMP server to the switch. The switch can then learn on which interfaces multicast members reside instead of flooding multicast traffic to all switch interfaces. (IGMP snooping is another method to constrain the flooding of multicast packets. For more information, see Chapter 23, “Configuring IGMP Snooping and MVR.”)

CGMP is necessary because the Layer 2 switch cannot distinguish between IP multicast data packets and IGMP report messages, which are both at the MAC-level and are addressed to the same group address. CGMP is mutually exclusive with HSRPv1. You cannot enable CGMP leaving processing and HSRPv1 at the same time. However, you can enable CGMP and HSRPv2 at the same time. For more information, see the “HSRP Versions” section on page 40-3.

**Configuring IP Multicast Routing**

These sections describe how to configure IP multicast routing:

- Default Multicast Routing Configuration, page 45-10
- Multicast Routing Configuration Guidelines, page 45-10
- Configuring Basic Multicast Routing, page 45-11 (required)
- Configuring PIM Stub Routing, page 45-13 (optional)
- Configuring Source-Specific Multicast, page 45-14
- Configuring Source Specific Multicast Mapping, page 45-18
- Configuring a Rendezvous Point, page 45-23 (required if the interface is in sparse-dense mode, and you want to treat the group as a sparse group)
- Using Auto-RP and a BSR, page 45-33 (required for non-Cisco PIMv2 devices to interoperate with Cisco PIM v1 devices)
- Monitoring the RP Mapping Information, page 45-34 (optional)
- Troubleshooting PIMv1 and PIMv2 Interoperability Problems, page 45-34 (optional)
Default Multicast Routing Configuration

Table 45-2 shows the default multicast routing configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multicast routing</td>
<td>Disabled on all interfaces.</td>
</tr>
<tr>
<td>PIM version</td>
<td>Version 2.</td>
</tr>
<tr>
<td>PIM mode</td>
<td>No mode is defined.</td>
</tr>
<tr>
<td>PIM RP address</td>
<td>None configured.</td>
</tr>
<tr>
<td>PIM domain border</td>
<td>Disabled.</td>
</tr>
<tr>
<td>PIM multicast boundary</td>
<td>None.</td>
</tr>
<tr>
<td>Candidate BSRs</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Candidate RPs</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Shortest-path tree threshold rate</td>
<td>0 kbps.</td>
</tr>
<tr>
<td>PIM router query message interval</td>
<td>30 seconds.</td>
</tr>
</tbody>
</table>

Multicast Routing Configuration Guidelines

To avoid misconfiguring multicast routing on your switch, review the information in these sections:
- PIMv1 and PIMv2 Interoperability, page 45-10
- Auto-RP and BSR Configuration Guidelines, page 45-11

PIMv1 and PIMv2 Interoperability

The Cisco PIMv2 implementation provides interoperability and transition between Version 1 and Version 2, although there might be some minor problems.

You can upgrade to PIMv2 incrementally. PIM Versions 1 and 2 can be configured on different routers and multilayer switches within one network. Internally, all routers and multilayer switches on a shared media network must run the same PIM version. Therefore, if a PIMv2 device detects a PIMv1 device, the Version 2 device downgrades itself to Version 1 until all Version 1 devices have been shut down or upgraded.

PIMv2 uses the BSR to discover and announce RP-set information for each group prefix to all the routers and multilayer switches in a PIM domain. PIMv1, together with the Auto-RP feature, can perform the same tasks as the PIMv2 BSR. However, Auto-RP is a standalone protocol, separate from PIMv1, and is a proprietary Cisco protocol. PIMv2 is a standards track protocol in the IETF. We recommend that you use PIMv2. The BSR mechanism interoperates with Auto-RP on Cisco routers and multilayer switches. For more information, see the “Auto-RP and BSR Configuration Guidelines” section on page 45-11.

When PIMv2 devices interoperate with PIMv1 devices, Auto-RP should have already been deployed. A PIMv2 BSR that is also an Auto-RP mapping agent automatically advertises the RP elected by Auto-RP. That is, Auto-RP sets its single RP on every router or multilayer switch in the group. Not all routers and switches in the domain use the PIMv2 hash function to select multiple RPs.

Dense-mode groups in a mixed PIMv1 and PIMv2 region need no special configuration; they automatically interoperate.
Sparse-mode groups in a mixed PIMv1 and PIMv2 region are possible because the Auto-RP feature in PIMv1 interoperates with the PIMv2 RP feature. Although all PIMv2 devices can also use PIMv1, we recommend that the RPs be upgraded to PIMv2. To ease the transition to PIMv2, we have these recommendations:

- Use Auto-RP throughout the region.
- Configure sparse-dense mode throughout the region.

If Auto-RP is not already configured in the PIMv1 regions, configure Auto-RP. For more information, see the “Configuring Auto-RP” section on page 45-25.

**Auto-RP and BSR Configuration Guidelines**

There are two approaches to using PIMv2. You can use Version 2 exclusively in your network or migrate to Version 2 by employing a mixed PIM version environment.

- If your network is all Cisco routers and multilayer switches, you can use either Auto-RP or BSR.
- If you have non-Cisco routers in your network, you must use BSR.
- If you have Cisco PIMv1 and PIMv2 routers and multilayer switches and non-Cisco routers, you must use both Auto-RP and BSR. If your network includes routers from other vendors, configure the Auto-RP mapping agent and the BSR on a Cisco PIMv2 device. Ensure that no PIMv1 device is located in the path between the BSR and a non-Cisco PIMv2 device.
- Because bootstrap messages are sent hop-by-hop, a PIMv1 device prevents these messages from reaching all routers and multilayer switches in your network. Therefore, if your network has a PIMv1 device in it and only Cisco routers and multilayer switches, it is best to use Auto-RP.
- If you have a network that includes non-Cisco routers, configure the Auto-RP mapping agent and the BSR on a Cisco PIMv2 router or multilayer switch. Ensure that no PIMv1 device is on the path between the BSR and a non-Cisco PIMv2 router.
- If you have non-Cisco PIMv2 routers that need to interoperate with Cisco PIMv1 routers and multilayer switches, both Auto-RP and a BSR are required. We recommend that a Cisco PIMv2 device be both the Auto-RP mapping agent and the BSR. For more information, see the “Using Auto-RP and a BSR” section on page 45-33.

**Configuring Basic Multicast Routing**

You must enable IP multicast routing and configure the PIM version and the PIM mode. Then the software can forward multicast packets, and the switch can populate its multicast routing table.

You can configure an interface to be in PIM dense mode, sparse mode, or sparse-dense mode. The switch populates its multicast routing table and forwards multicast packets it receives from its directly connected LANs according to the mode setting. You must enable PIM in one of these modes for an interface to perform IP multicast routing. Enabling PIM on an interface also enables IGMP operation on that interface.

---

**Note**

If you enable PIM on multiple interfaces, when most of them are not on the outgoing interface list, and IGMP snooping is disabled, the outgoing interface might not be able to sustain line rate for multicast traffic because of the extra replication.
In populating the multicast routing table, dense-mode interfaces are always added to the table. Sparse-mode interfaces are added to the table only when periodic join messages are received from downstream devices or when there is a directly connected member on the interface. When forwarding from a LAN, sparse-mode operation occurs if there is an RP known for the group. If so, the packets are encapsulated and sent toward the RP. When no RP is known, the packet is flooded in a dense-mode fashion. If the multicast traffic from a specific source is sufficient, the receiver’s first-hop router might send join messages toward the source to build a source-based distribution tree.

By default, multicast routing is disabled, and there is no default mode setting. This procedure is required. Beginning in privileged EXEC mode, follow these steps to enable IP multicasting, to configure a PIM version, and to configure a PIM mode. This procedure is required.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code> Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>ip multicast-routing distributed</code> Enable IP multicast distributed switching.</td>
</tr>
</tbody>
</table>
| Step 3  | `interface interface-id` Specify the Layer 3 interface on which you want to enable multicast routing, and enter interface configuration mode. The specified interface must be one of the following:  
- A routed port: a physical port that has been configured as a Layer 3 port by entering the `no switchport` interface configuration command.  
- An SVI: a VLAN interface created by using the `interface vlan vlan-id` global configuration command.  
-  
These interfaces must have IP addresses assigned to them. For more information, see the “Configuring Layer 3 Interfaces” section on page 9-17. |
| Step 4  | `ip pim version [1 | 2]` Configure the PIM version on the interface.  
By default, Version 2 is enabled and is the recommended setting.  
An interface in PIMv2 mode automatically downgrades to PIMv1 mode if that interface has a PIMv1 neighbor. The interface returns to Version 2 mode after all Version 1 neighbors are shut down or upgraded.  
For more information, see the “PIMv1 and PIMv2 Interoperability” section on page 45-10. |
By default, no mode is configured.  
The keywords have these meanings:  
- `dense-mode`—Enables dense mode of operation.  
- `sparse-mode`—Enables sparse mode of operation. If you configure sparse-mode, you must also configure an RP. For more information, see the “Configuring a Rendezvous Point” section on page 45-23.  
- `sparse-dense-mode`—Causes the interface to be treated in the mode in which the group belongs. Sparse-dense-mode is the recommended setting. |
Configuring PIM Stub Routing

The PIM Stub routing feature supports multicast routing between the distribution layer and the access layer. It supports two types of PIM interfaces, uplink PIM interfaces, and PIM passive interfaces. A routed interface configured with the PIM passive mode does not pass or forward PIM control traffic, it only passes and forwards IGMP traffic.

PIM Stub Routing Configuration Guidelines

Follow these guidelines when enabling PIM stub routing on an interface:

- Before configuring PIM stub routing, you must have IP multicast routing configured on both the stub router and the central router. You must also have PIM mode (dense-mode, sparse-mode, or dense-sparse-mode) configured on the uplink interface of the stub router.
- The PIM stub router does not route the transit traffic between the distribution routers. Unicast (EIGRP) stub routing enforces this behavior. You must configure unicast stub routing to assist the PIM stub router behavior. For more information, see the “Configuring EIGRP Stub Routing” section on page 36-41.
- Only directly connected multicast (IGMP) receivers and sources are allowed in the Layer 2 access domains. The PIM protocol is not supported in access domains.
- The redundant PIM stub router topology is not supported.

Enabling PIM Stub Routing

Beginning in privileged EXEC mode, follow these steps to enable PIM stub routing on an interface. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>ip pim passive</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
</tr>
<tr>
<td>Step 5</td>
<td>show ip pim interface</td>
</tr>
<tr>
<td>Step 6</td>
<td>show running-config</td>
</tr>
<tr>
<td>Step 7</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To disable multicasting, use the **no ip multicast-routing distributed** global configuration command. To return to the default PIM version, use the **no ip pim version** interface configuration command. To disable PIM on an interface, use the **no ip pim** interface configuration command.
To disable PIM stub routing on an interface, use the **no ip pim passive** interface configuration command.

In this example, IP multicast routing is enabled, Switch A PIM uplink port 25 is configured as a routed uplink port with **spare-dense-mode enabled**. PIM stub routing is enabled on the VLAN 100 interfaces and on Gigabit Ethernet port 20 in **Figure 45-2**:

```
Switch(config)# ip multicast-routing distributed
Switch(config)# interface GigabitEthernet1/0/25
Switch(config-if)# no switchport
Switch(config-if)# ip address 3.1.1.2 255.255.255.0
Switch(config-if)# ip pim sparse-dense-mode
Switch(config-if)# exit
Switch(config)# interface vlan100
Switch(config-if)# ip pim passive
Switch(config-if)# exit
Switch(config)# interface GigabitEthernet1/0/20
Switch(config-if)# ip address 100.1.1.1 255.255.255.0
Switch(config-if)# ip pim passive
Switch(config-if)# exit
Switch(config)# interface vlan100
Switch(config-if)# ip address 10.1.1.1 255.255.255.0
Switch(config-if)# ip pim passive
Switch(config-if)# end
```

To verify that PIM stub is enabled for each interface, use the **show ip pim interface** privileged EXEC command:

```
Switch# show ip pim interface
Address   Interface   Ver/Nbr Query DR   DR
          Mode       Count Intvl Prior
3.1.1.2    GigabitEth  v2/SD   1 30 1 3.1.1.2
100.1.1.1  Vlan100     v2/P    0 30 1 100.1.1.1
10.1.1.1   GigabitEth  v2/P    0 30 1 10.1.1.1
```

Use these privileged EXEC commands to display information about PIM stub configuration and status:

- **show ip pim interface** displays the PIM stub that is enabled on each interface.
- **show ip igmp detail** displays the interested clients that have joined the specific multicast source group.
- **show ip igmp mroute** verifies that the multicast stream forwards from the source to the interested clients.

### Configuring Source-Specific Multicast

This section describes how to configure source-specific multicast (SSM). For a complete description of the SSM commands in this section, refer to the *Cisco IP Multicast Command Reference*:


To locate documentation for other commands that appear in this chapter, use the command reference master index, or search online.

The SSM feature is an extension of IP multicast in which datagram traffic is forwarded to receivers from only those multicast sources that the receivers have explicitly joined. For multicast groups configured for SSM, only SSM distribution trees (no shared trees) are created.
SSM Components Overview

SSM is a datagram delivery model that best supports one-to-many applications, also known as broadcast applications. SSM is a core networking technology for the Cisco implementation of IP multicast solutions targeted for audio and video broadcast application environments. The switch supports these components that support the implementation of SSM:

- Protocol independent multicast source-specific mode (PIM-SSM)
  PIM-SSM is the routing protocol that supports the implementation of SSM and is derived from PIM sparse mode (PIM-SM).
- Internet Group Management Protocol version 3 (IGMPv3)
  To run SSM with IGMPv3, SSM must be supported in the Cisco IOS router, the host where the application is running, and the application itself.

How SSM Differs from Internet Standard Multicast

The current IP multicast infrastructure in the Internet and many enterprise intranets are based on the PIM-SM protocol and Multicast Source Discovery Protocol (MSDP). These protocols have the limitations of the Internet Standard Multicast (ISM) service model. For example, with ISM, the network must maintain knowledge about which hosts in the network are actively sending multicast traffic.

The ISM service consists of the delivery of IP datagrams from any source to a group of receivers called the multicast host group. The datagram traffic for the multicast host group consists of datagrams with an arbitrary IP unicast source address S and the multicast group address G as the IP destination address. Systems receive this traffic by becoming members of the host group.

Membership in a host group simply requires signalling the host group through IGMP version 1, 2, or 3. In SSM, delivery of datagrams is based on (S, G) channels. In both SSM and ISM, no signalling is required to become a source. However, in SSM, receivers must subscribe or unsubscribe to (S, G) channels to receive or not receive traffic from specific sources. In other words, receivers can receive traffic only from (S, G) channels to which they are subscribed, whereas in ISM, receivers need not know the IP addresses of sources from which they receive their traffic. The proposed standard approach for channel subscription signalling use IGMP include mode membership reports, which are supported only in IGMP version 3.

SSM IP Address Range

SSM can coexist with the ISM service by applying the SSM delivery model to a configured subset of the IP multicast group address range. Cisco IOS software allows SSM configuration for the IP multicast address range of 224.0.0.0 through 239.255.255.255. When an SSM range is defined, existing IP multicast receiver applications do not receive any traffic when they try to use an address in the SSM range (unless the application is modified to use an explicit (S, G) channel subscription).

SSM Operations

An established network, in which IP multicast service is based on PIM-SM, can support SSM services. SSM can also be deployed alone in a network without the full range of protocols that are required for interdomain PIM-SM (for example, MSDP, Auto-RP, or bootstrap router [BSR]) if only SSM service is needed.
If SSM is deployed in a network already configured for PIM-SM, only the last-hop routers support SSM. Routers that are not directly connected to receivers do not require support for SSM. In general, these not-last-hop routers must only run PIM-SM in the SSM range and might need additional access control configuration to suppress MSDP signalling, registering, or PIM-SM shared tree operations from occurring within the SSM range.

Use the `ip pim ssm` global configuration command to configure the SSM range and to enable SSM. This configuration has the following effects:

- For groups within the SSM range, (S, G) channel subscriptions are accepted through IGMPv3 include-mode membership reports.
- PIM operations within the SSM range of addresses change to PIM-SSM, a mode derived from PIM-SM. In this mode, only PIM (S, G) join and prune messages are generated by the router, and no (S, G) rendezvous point tree (RPT) or (*, G) RPT messages are generated. Incoming messages related to RPT operations are ignored or rejected, and incoming PIM register messages are immediately answered with register-stop messages. PIM-SSM is backward-compatible with PIM-SM unless a router is a last-hop router. Therefore, routers that are not last-hop routers can run PIM-SM for SSM groups (for example, if they do not yet support SSM).
- No MSDP source-active (SA) messages within the SSM range are accepted, generated, or forwarded.

**IGMPv3 Host Signalling**

In IGMPv3, hosts signal membership to last hop routers of multicast groups. Hosts can signal group membership with filtering capabilities with respect to sources. A host can either signal that it wants to receive traffic from all sources sending to a group except for some specific sources (called exclude mode), or that it wants to receive traffic only from some specific sources sending to the group (called include mode).

IGMPv3 can operate with both ISM and SSM. In ISM, both exclude and include mode reports are applicable. In SSM, only include mode reports are accepted by the last-hop router. Exclude mode reports are ignored.

**Configuration Guidelines**

This section contains the guidelines for configuring SSM.

**Legacy Applications Within the SSM Range Restrictions**

Existing applications in a network predating SSM do not work within the SSM range unless they are modified to support (S, G) channel subscriptions. Therefore, enabling SSM in a network can cause problems for existing applications if they use addresses within the designated SSM range.

**Address Management Restrictions**

Address management is still necessary to some degree when SSM is used with Layer 2 switching mechanisms. Cisco Group Management Protocol (CGMP), IGMP snooping, or Router-Port Group Management Protocol (RGMP) support only group-specific filtering, not (S, G) channel-specific filtering. If different receivers in a switched network request different (S, G) channels sharing the same group, they do not benefit from these existing mechanisms. Instead, both receivers receive all (S, G) channel traffic and filter out the unwanted traffic on input. Because SSM can re-use the group addresses in the SSM range for many independent applications, this situation can lead to decreased traffic filtering in a switched network. For this reason, it is important to use random IP addresses from the SSM range.
for an application to minimize the chance for re-use of a single address within the SSM range between different applications. For example, an application service providing a set of television channels should, even with SSM, use a different group for each television (S, G) channel. This setup guarantees that multiple receivers to different channels within the same application service never experience traffic aliasing in networks that include Layer 2 switches.

**IGMP Snooping and CGMP Limitations**

IGMPv3 uses new membership report messages that might not be correctly recognized by older IGMP snooping switches.

For more information about switching issues related to IGMP (especially with CGMP), refer to the “Configuring IGMP Version 3” section of the “Configuring IP Multicast Routing” chapter.

**State Maintenance Limitations**

In PIM-SSM, the last hop router continues to periodically send (S, G) join messages if appropriate (S, G) subscriptions are on the interfaces. Therefore, as long as receivers send (S, G) subscriptions, the shortest path tree (SPT) state from the receivers to the source is maintained, even if the source does not send traffic for longer periods of time (or even never).

This case is opposite to PIM-SM, where (S, G) state is maintained only if the source is sending traffic and receivers are joining the group. If a source stops sending traffic for more than 3 minutes in PIM-SM, the (S, G) state is deleted and only re-established after packets from the source arrive again through the RPT. Because no mechanism in PIM-SSM notifies a receiver that a source is active, the network must maintain the (S, G) state in PIM-SSM as long as receivers are requesting receipt of that channel.

**Configuring SSM**

Beginning in privileged EXEC mode, follow these steps to configure SSM:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>ip pim ssm [default</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface type number Select an interface that is connected to hosts on which IGMPv3 can be enabled, and enter the interface configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>ip pim {sparse-mode</td>
</tr>
<tr>
<td>Step 4</td>
<td>ip igmp version 3 Enable IGMPv3 on this interface. The default version of IGMP is set to Version 2.</td>
</tr>
</tbody>
</table>

**Monitoring SSM**

Beginning in privileged EXEC mode, follow these steps to monitor SSM.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router# show ip igmp groups detail Display the (S, G) channel subscription through IGMPv3.</td>
<td></td>
</tr>
<tr>
<td>Router# show ip mroute Display whether a multicast group supports SSM service or whether a source-specific host report was received.</td>
<td></td>
</tr>
</tbody>
</table>
Configuring Source Specific Multicast Mapping

The Source Specific Multicast (SSM) mapping feature supports SSM transition when supporting SSM on the end system is impossible or unwanted due to administrative or technical reasons. You can use SSM mapping to leverage SSM for video delivery to legacy STBs that do not support IGMPv3 or for applications that do not use the IGMPv3 host stack.

This section covers these topics:

- Configuration Guidelines, page 45-18
- SSM Mapping Overview, page 45-18
- Configuring SSM Mapping, page 45-20
- Monitoring SSM Mapping, page 45-23

Configuration Guidelines

These are the SSM mapping configuration guidelines:

- Before you configure SSM mapping, enable IP multicast routing, enable PIM sparse mode, and configure SSM. For information on enabling IP multicast routing and PIM sparse mode, see the “Default Multicast Routing Configuration” section on page 45-10.

- Before you configure static SSM mapping, you must configure access control lists (ACLs) that define the group ranges to be mapped to source addresses. For information on configuring an ACL, see Chapter 33, “Configuring Network Security with ACLs.”

- Before you can configure and use SSM mapping with DNS lookups, you must be able to add records to a running DNS server. If you do not already have a DNS server running, you need to install one. You can use a product such as Cisco Network Registrar. Go to this URL for more information: http://www.cisco.com/en/US/products/sw/netmgtsw/ps1982/index.html

These are the SSM mapping restrictions:

- The SSM mapping feature does not have all the benefits of full SSM. Because SSM mapping takes a group join from a host and identifies this group with an application associated with one or more sources, it can only support one such application per group. Full SSM applications can still share the same group as in SSM mapping.

- Enable IGMPv3 with care on the last hop router when you rely solely on SSM mapping as a transition solution for full SSM. When you enable both SSM mapping and IGMPv3 and the hosts already support IGMPv3 (but not SSM), the hosts send IGMPv3 group reports. SSM mapping does not support these IGMPv3 group reports, and the router does not correctly associate sources with these reports.

SSM Mapping Overview

In a typical STB deployment, each TV channel uses one separate IP multicast group and has one active server host sending the TV channel. A single server can send multiple TV channels, but each to a different group. In this network environment, if a router receives an IGMPv1 or IGMPv2 membership report for a particular group, the report addresses the well-known TV server for the TV channel associated with the multicast group.

When SSM mapping is configured, if a router receives an IGMPv1 or IGMPv2 membership report for a particular group, the router translates this report into one or more channel memberships for the well-known sources associated with this group.
When the router receives an IGMPv1 or IGMPv2 membership report for a group, the router uses SSM mapping to determine one or more source IP addresses for the group. SSM mapping then translates the membership report as an IGMPv3 report and continues as if it had received an IGMPv3 report. The router then sends PIM joins and continues to be joined to these groups as long as it continues to receive the IGMPv1 or IGMPv2 membership reports, and the SSM mapping for the group remains the same.

SSM mapping enables the last hop router to determine the source addresses either by a statically configured table on the router or through a DNS server. When the statically configured table or the DNS mapping changes, the router leaves the current sources associated with the joined groups.

Go to this URL for additional information on SSM mapping:


**Static SSM Mapping**

With static SSM mapping, you can configure the last hop router to use a static map to determine the sources that are sending to groups. Static SSM mapping requires that you configure ACLs to define group ranges. Then you can map the groups permitted by those ACLs to sources by using the `ip igmp static ssm-map` global configuration command.

You can configure static SSM mapping in smaller networks when a DNS is not needed or to locally override DNS mappings. When configured, static SSM mappings take precedence over DNS mappings.

**DNS-Based SSM Mapping**

You can use DNS-based SSM mapping to configure the last hop router to perform a reverse DNS lookup to determine sources sending to groups. When DNS-based SSM mapping is configured, the router constructs a domain name that includes the group address and performs a reverse lookup into the DNS. The router looks up IP address resource records and uses them as the source addresses associated with this group. SSM mapping supports up to 20 sources for each group. The router joins all sources configured for a group (see Figure 45-4).
Configuring IP Multicast Routing

Figure 45-4  DNS-Based SSM-Mapping

The SSM mapping mechanism that enables the last hop router to join multiple sources for a group can provide source redundancy for a TV broadcast. In this context, the last hop router provides redundancy using SSM mapping to simultaneously join two video sources for the same TV channel. However, to prevent the last hop router from duplicating the video traffic, the video sources must use a server-side switchover mechanism. One video source is active, and the other backup video source is passive. The passive source waits until an active source failure is detected before sending the video traffic for the TV channel. Thus, the server-side switchover mechanism ensures that only one of the servers is actively sending video traffic for the TV channel.

To look up one or more source addresses for a group that includes G1, G2, G3, and G4, you must configure these DNS records on the DNS server:

```
    IN A source-address-2
    IN A source-address-n
```

Refer to your DNS server documentation for more information about configuring DNS resource records, and go to this URL for additional information on SSM mapping:


Configuring SSM Mapping

This section covers these topics:

- Configuring Static SSM Mapping, page 45-21 (required)
- Configuring DNS-Based SSM Mapping, page 45-21 (required)
- Configuring Static Traffic Forwarding with SSM Mapping, page 45-22 (optional)
Configuring Static SSM Mapping

Beginning in privileged EXEC mode, follow these steps to configure static SSM mapping:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip igmp ssm-map enable</td>
</tr>
<tr>
<td>Step 3</td>
<td>no ip igmp ssm-map query dns</td>
</tr>
<tr>
<td>Step 4</td>
<td>ip igmp ssm-map static access-list source-address</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>Repeat Step 4 to configure additional static SSM mappings, if required.</td>
</tr>
<tr>
<td>Step 6</td>
<td>end</td>
</tr>
<tr>
<td>Step 7</td>
<td>show running-config</td>
</tr>
<tr>
<td>Step 8</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

Go to this URL to see SSM mapping configuration examples:


Configuring DNS-Based SSM Mapping

To configure DNS-based SSM mapping, you need to create a DNS server zone or add records to an existing zone. If the routers that are using DNS-based SSM mapping are also using DNS for other purposes, you should use a normally configured DNS server. If DNS-based SSM mapping is the only DNS implementation being used on the router, you can configure a false DNS setup with an empty root zone or a root zone that points back to itself.

Beginning in privileged EXEC mode, follow these steps to configure DNS-based SSM mapping:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip igmp ssm-map enable</td>
</tr>
</tbody>
</table>
Configuring Static Traffic Forwarding with SSM Mapping

Use static traffic forwarding with SSM mapping to statically forward SSM traffic for certain groups. Beginning in privileged EXEC mode, follow these steps to configure static traffic forwarding with SSM mapping:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>interface type number</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>ip igmp static-group group-address source ssm-map</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>show running-config</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>
Monitoring SSM Mapping

Use the privileged EXEC commands in Table 45-3 to monitor SSM mapping.

Table 45-3 SSM Mapping Monitoring Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip igmp ssm-mapping</td>
<td>Display information about SSM mapping.</td>
</tr>
<tr>
<td>show ip igmp ssm-mapping group-address</td>
<td>Display the sources that SSM mapping uses for a particular group.</td>
</tr>
<tr>
<td>show ip igmp groups [group-name</td>
<td>group-address</td>
</tr>
<tr>
<td>show host</td>
<td>Display the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses.</td>
</tr>
<tr>
<td>debug ip igmp group-address</td>
<td>Display the IGMP packets received and sent and IGMP host-related events.</td>
</tr>
</tbody>
</table>

Go to this URL to see SSM mapping monitoring examples:

Configuring a Rendezvous Point

You must have an RP if the interface is in sparse-dense mode and if you want to treat the group as a sparse group. You can use several methods, as described in these sections:

- Manually Assigning an RP to Multicast Groups, page 45-23
- Configuring Auto-RP, page 45-25 (a standalone, Cisco-proprietary protocol separate from PIMv1)
- Configuring PIMv2 BSR, page 45-29 (a standards track protocol in the IETF)

You can use Auto-RP, BSR, or a combination of both, depending on the PIM version you are running and the types of routers in your network. For more information, see the “PIMv1 and PIMv2 Interoperability” section on page 45-10 and the “Auto-RP and BSR Configuration Guidelines” section on page 45-11.

Manually Assigning an RP to Multicast Groups

This section explains how to manually configure an RP. If the RP for a group is learned through a dynamic mechanism (such as Auto-RP or BSR), you need not perform this task for that RP.

Senders of multicast traffic announce their existence through register messages received from the source’s first-hop router (designated router) and forwarded to the RP. Receivers of multicast packets use RPs to join a multicast group by using explicit join messages. RPs are not members of the multicast group; rather, they serve as a meeting place for multicast sources and group members.

You can configure a single RP for multiple groups defined by an access list. If there is no RP configured for a group, the multilayer switch treats the group as dense and uses the dense-mode PIM techniques.
Beginning in privileged EXEC mode, follow these steps to manually configure the address of the RP. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>ip pim rp-address ip-address [access-list-number] [override]</td>
</tr>
<tr>
<td></td>
<td>Configure the address of a PIM RP. By default, no PIM RP address is configured. You must configure the IP address of RPs on all routers and multilayer switches (including the RP). If there is no RP configured for a group, the switch treats the group as dense, using the dense-mode PIM techniques. A PIM device can be an RP for more than one group. Only one RP address can be used at a time within a PIM domain. The access-list conditions specify for which groups the device is an RP.</td>
</tr>
<tr>
<td></td>
<td>• For <em>ip-address</em>, enter the unicast address of the RP in dotted-decimal notation.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) For <em>access-list-number</em>, enter an IP standard access list number from 1 to 99. If no access list is configured, the RP is used for all groups.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) The <strong>override</strong> keyword means that if there is a conflict between the RP configured with this command and one learned by Auto-RP or BSR, the RP configured with this command prevails.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>access-list access-list-number {deny</td>
</tr>
<tr>
<td></td>
<td>Create a standard access list, repeating the command as many times as necessary.</td>
</tr>
<tr>
<td></td>
<td>• For <em>access-list-number</em>, enter the access list number specified in Step 2.</td>
</tr>
<tr>
<td></td>
<td>• The <strong>deny</strong> keyword denies access if the conditions are matched. The <strong>permit</strong> keyword permits access if the conditions are matched.</td>
</tr>
<tr>
<td></td>
<td>• For <em>source</em>, enter the multicast group address for which the RP should be used.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) For <em>source-wildcard</em>, enter the wildcard bits in dotted decimal notation to be applied to the source. Place ones in the bit positions that you want to ignore. Recall that the access list is always terminated by an implicit deny statement for everything.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>end</td>
</tr>
<tr>
<td></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>show running-config</td>
</tr>
<tr>
<td></td>
<td>Verify your entries.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>copy running-config startup-config</td>
</tr>
<tr>
<td></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To remove an RP address, use the `no ip pim rp-address ip-address [access-list-number] [override]` global configuration command.

This example shows how to configure the address of the RP to 147.106.6.22 for multicast group 225.2.2.2 only:

```
Switch(config)# access-list 1 permit 225.2.2.2 0.0.0.0
Switch(config)# ip pim rp-address 147.106.6.22 1
```
Configuring Auto-RP

Auto-RP uses IP multicast to automate the distribution of group-to-RP mappings to all Cisco routers and multilayer switches in a PIM network. It has these benefits:

- It is easy to use multiple RPs within a network to serve different group ranges.
- It provides load splitting among different RPs and arrangement of RPs according to the location of group participants.
- It avoids inconsistent, manual RP configurations on every router and multilayer switch in a PIM network, which can cause connectivity problems.

**Note**
If you configure PIM in sparse mode or sparse-dense mode and do not configure Auto-RP, you must manually configure an RP as described in the “Manually Assigning an RP to Multicast Groups” section on page 45-23.

**Note**
If routed ports are configured in sparse mode, Auto-RP can still be used if all devices are configured with a manual RP address for the Auto-RP groups.

These sections describe how to configure Auto-RP:

- Setting up Auto-RP in a New Internetwork, page 45-25 (optional)
- Adding Auto-RP to an Existing Sparse-Mode Cloud, page 45-25 (optional)
- Preventing Join Messages to False RPs, page 45-27 (optional)
- Filtering Incoming RP Announcement Messages, page 45-28 (optional)

For overview information, see the “Auto-RP” section on page 45-6.

Setting up Auto-RP in a New Internetwork

If you are setting up Auto-RP in a new internetwork, you do not need a default RP because you configure all the interfaces for sparse-dense mode. Follow the process described in the next section “Adding Auto-RP to an Existing Sparse-Mode Cloud” section on page 45-25. However, skip Step 3 to configure a PIM router as the RP for the local group.

Adding Auto-RP to an Existing Sparse-Mode Cloud

This section contains some suggestions for the initial deployment of Auto-RP into an existing sparse-mode cloud to minimize disruption of the existing multicast infrastructure.
Beginning in privileged EXEC mode, follow these steps to deploy Auto-RP in an existing sparse-mode cloud. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**                       | **show running-config** Verify that a default RP is already configured on all PIM devices and the RP in the sparse-mode network. It was previously configured with the ip pim rp-address global configuration command.  
This step is not required for spare-dense-mode environments.  
The selected RP should have good connectivity and be available across the network. Use this RP for the global groups (for example 224.x.x.x and other global groups). Do not reconfigure the group address range that this RP serves. RPs dynamically discovered through Auto-RP take precedence over statically configured RPs. Assume that it is desirable to use a second RP for the local groups. |
| **Step 2**                       | **configure terminal** Enter global configuration mode.                                                                                                                                                  |
| **Step 3**                       | **ip pim send-rp-announce** interface-id scope ttl group-list access-list-number interval seconds** Configure another PIM device to be the candidate RP for local groups.  
• For interface-id, enter the interface type and number that identifies the RP address. Valid interfaces include physical ports, port channels, and VLANs.  
• For scope ttl, specify the time-to-live value in hops. Enter a hop count that is high enough so that the RP-announce messages reach all mapping agents in the network. There is no default setting. The range is 1 to 255.  
• For group-list access-list-number, enter an IP standard access list number from 1 to 99. If no access list is configured, the RP is used for all groups.  
• For interval seconds, specify how often the announcement messages must be sent. The default is 60 seconds. The range is 1 to 16383. |
| **Step 4**                       | **access-list access-list-number {deny | permit} source [source-wildcard]** Create a standard access list, repeating the command as many times as necessary.  
• For access-list-number, enter the access list number specified in Step 3.  
• The deny keyword denies access if the conditions are matched. The permit keyword permits access if the conditions are matched.  
• For source, enter the multicast group address range for which the RP should be used.  
• (Optional) For source-wildcard, enter the wildcard bits in dotted decimal notation to be applied to the source. Place ones in the bit positions that you want to ignore.  
Recall that the access list is always terminated by an implicit deny statement for everything. |
**Chapter 45 Configuring IP Multicast Routing**

**Configuring IP Multicast Routing**

To remove the PIM device configured as the candidate RP, use the `no ip pim send-rp-announce` interface-id global configuration command. To remove the switch as the RP-mapping agent, use the `no ip pim send-rp-discovery` global configuration command.

This example shows how to send RP announcements out all PIM-enabled ports for a maximum of 31 hops. The IP address of port 1 is the RP. Access list 5 describes the group for which this switch serves as RP:

```
Switch(config)# ip pim send-rp-announce gigabitethernet1/0/1 scope 31 group-list 5
Switch(config)# access-list 5 permit 224.0.0.0 15.255.255.255
```

**Preventing Join Messages to False RPs**

Find whether the `ip pim accept-rp` command was previously configured throughout the network by using the `show running-config` privileged EXEC command. If the `ip pim accept-rp` command is not configured on any device, this problem can be addressed later. In those routers or multilayer switches already configured with the `ip pim accept-rp` command, you must enter the command again to accept the newly advertised RP.

To accept all RPs advertised with Auto-RP and reject all other RPs by default, use the `ip pim accept-rp auto-rp` global configuration command. This procedure is optional.

To remove the PIM device configured as the candidate RP, use the `no ip pim send-rp-announce` interface-id global configuration command. To remove the switch as the RP-mapping agent, use the `no ip pim send-rp-discovery` global configuration command.

This example shows how to send RP announcements out all PIM-enabled ports for a maximum of 31 hops. The IP address of port 1 is the RP. Access list 5 describes the group for which this switch serves as RP:

```
Switch(config)# ip pim send-rp-announce gigabitethernet1/0/1 scope 31 group-list 5
Switch(config)# access-list 5 permit 224.0.0.0 15.255.255.255
```

Find whether the `ip pim accept-rp` command was previously configured throughout the network by using the `show running-config` privileged EXEC command. If the `ip pim accept-rp` command is not configured on any device, this problem can be addressed later. In those routers or multilayer switches already configured with the `ip pim accept-rp` command, you must enter the command again to accept the newly advertised RP.

To accept all RPs advertised with Auto-RP and reject all other RPs by default, use the `ip pim accept-rp auto-rp` global configuration command. This procedure is optional.

If all ports are in sparse mode, use a default-configured RP to support the two well-known groups 224.0.1.39 and 224.0.1.40. Auto-RP uses these two well-known groups to collect and distribute RP-mapping information. When this is the case and the `ip pim accept-rp auto-rp` command is configured, another `ip pim accept-rp` command accepting the RP must be configured as follows:

```
Switch(config)# ip pim accept-rp 172.10.20.1 1
Switch(config)# access-list 1 permit 224.0.0.0 15.255.255.255
Switch(config)# access-list 1 permit 224.0.1.39
Switch(config)# access-list 1 permit 224.0.1.40
```
Filtering Incoming RP Announcement Messages

You can add configuration commands to the mapping agents to prevent a maliciously configured router from masquerading as a candidate RP and causing problems.

Beginning in privileged EXEC mode, follow these steps to filter incoming RP announcement messages. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>ip pim rp-announce-filter rp-list access-list-number group-list access-list-number</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>access-list access-list-number [deny</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>show running-config</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To remove a filter on incoming RP announcement messages, use the **no ip pim rp-announce-filter rp-list access-list-number [group-list access-list-number]** global configuration command.
This example shows a sample configuration on an Auto-RP mapping agent that is used to prevent candidate RP announcements from being accepted from unauthorized candidate RPs:

```plaintext
Switch(config)# ip pim rp-announce-filter rp-list 10 group-list 20
Switch(config)# access-list 10 permit host 172.16.5.1
Switch(config)# access-list 10 permit host 172.16.2.1
Switch(config)# access-list 20 deny 239.0.0.0 0.0.255.255
Switch(config)# access-list 20 permit 224.0.0.0 15.255.255.255
```

In this example, the mapping agent accepts candidate RP announcements from only two devices, 172.16.5.1 and 172.16.2.1. The mapping agent accepts candidate RP announcements from these two devices only for multicast groups that fall in the group range of 224.0.0.0 to 239.255.255.255. The mapping agent does not accept candidate RP announcements from any other devices in the network. Furthermore, the mapping agent does not accept candidate RP announcements from 172.16.5.1 or 172.16.2.1 if the announcements are for any groups in the 239.0.0.0 through 239.255.255.255 range. This range is the administratively scoped address range.

**Configuring PIMv2 BSR**

These sections describe how to set up BSR in your PIMv2 network:

- Defining the PIM Domain Border, page 45-29 (optional)
- Defining the IP Multicast Boundary, page 45-30 (optional)
- Configuring Candidate BSRs, page 45-31 (optional)
- Configuring Candidate RPs, page 45-32 (optional)

For overview information, see the “Bootstrap Router” section on page 45-7.

**Defining the PIM Domain Border**

As IP multicast becomes more widespread, the chance of one PIMv2 domain bordering another PIMv2 domain is increasing. Because these two domains probably do not share the same set of RPs, BSR, candidate RPs, and candidate BSRs, you need to constrain PIMv2 BSR messages from flowing into or out of the domain. Allowing these messages to leak across the domain borders could adversely affect the normal BSR election mechanism and elect a single BSR across all bordering domains and co-mingle candidate RP advertisements, resulting in the election of RPs in the wrong domain.

Beginning in privileged EXEC mode, follow these steps to define the PIM domain border. This procedure is optional.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>interface interface-id</td>
<td>Specify the interface to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>3</td>
<td>ip pim bsr-border</td>
<td>Define a PIM bootstrap message boundary for the PIM domain. Enter this command on each interface that connects to other bordering PIM domains. This command instructs the switch to neither send or receive PIMv2 BSR messages on this interface as shown in Figure 45-5.</td>
</tr>
<tr>
<td>4</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>5</td>
<td>show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>6</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
To remove the PIM border, use the `no ip pim bsr-border` interface configuration command.

**Figure 45-5 Constrainin g PIMv2 BSR Messages**

**Defining the IP Multicast Boundary**

You define a multicast boundary to prevent Auto-RP messages from entering the PIM domain. You create an access list to deny packets destined for 224.0.1.39 and 224.0.1.40, which carry Auto-RP information.

Beginning in privileged EXEC mode, follow these steps to define a multicast boundary. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>access-list access-list-number deny source [source-wildcard]</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>ip multicast boundary access-list-number</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>show running-config</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>
To remove the boundary, use the `no ip multicast boundary` interface configuration command.

This example shows a portion of an IP multicast boundary configuration that denies Auto-RP information:

```
Switch(config)# access-list 1 deny 224.0.1.39
Switch(config)# access-list 1 deny 224.0.1.40
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip multicast boundary 1
```

### Configuring Candidate BSRs

You can configure one or more candidate BSRs. The devices serving as candidate BSRs should have good connectivity to other devices and be in the backbone portion of the network.

Beginning in privileged EXEC mode, follow these steps to configure your switch as a candidate BSR. This procedure is optional.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td><code>ip pim bsr-candidate interface-id hash-mask-length [priority]</code></td>
<td>Configure your switch to be a candidate BSR.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For <code>interface-id</code>, enter the interface on this switch from which the BSR address is derived to make it a candidate. This interface must be enabled with PIM. Valid interfaces include physical ports, port channels, and VLANs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For <code>hash-mask-length</code>, specify the mask length (32 bits maximum) that is to be ANDed with the group address before the hash function is called. All groups with the same seed hash correspond to the same RP. For example, if this value is 24, only the first 24 bits of the group addresses matter.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) For <code>priority</code>, enter a number from 0 to 255. The BSR with the larger priority is preferred. If the priority values are the same, the device with the highest IP address is selected as the BSR. The default is 0.</td>
</tr>
<tr>
<td>3</td>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>4</td>
<td><code>show running-config</code></td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>5</td>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To remove this device as a candidate BSR, use the `no ip pim bsr-candidate` global configuration command.

This example shows how to configure a candidate BSR, which uses the IP address 172.21.24.18 on a port as the advertised BSR address, uses 30 bits as the hash-mask-length, and has a priority of 10.

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# ip address 172.21.24.18 255.255.255.0
Switch(config-if)# ip pim sparse-dense-mode
Switch(config-if)# ip pim bsr-candidate gigabitethernet1/0/2 30 10
```
Configuring Candidate RPs

You can configure one or more candidate RPs. Similar to BSRs, the RPs should also have good connectivity to other devices and be in the backbone portion of the network. An RP can serve the entire IP multicast address space or an interface on it. Candidate RPs send candidate RP advertisements to the BSR. When deciding which devices should be RPs, consider these options:

- In a network of Cisco routers and multilayer switches where only Auto-RP is used, any device can be configured as an RP.
- In a network that includes only Cisco PIMv2 routers and multilayer switches and with routers from other vendors, any device can be used as an RP.
- In a network of Cisco PIMv1 routers, Cisco PIMv2 routers, and routers from other vendors, configure only Cisco PIMv2 routers and multilayer switches as RPs.

Beginning in privileged EXEC mode, follow these steps to configure your switch to advertise itself as a PIMv2 candidate RP to the BSR. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>ip pim rp-candidate interface-id [group-list access-list-number]</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>access-list access-list-number {deny</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>show running-config</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To remove this device as a candidate RP, use the `no ip pim rp-candidate interface-id` global configuration command.
This example shows how to configure the switch to advertise itself as a candidate RP to the BSR in its PIM domain. Standard access list number 4 specifies the group prefix associated with the RP that has the address identified by a port. That RP is responsible for the groups with the prefix 239.

```
Switch(config)# ip pim rp-candidate gigabitethernet1/0/2 group-list 4
Switch(config)# access-list 4 permit 239.0.0.0 0.255.255.255
```

**Using Auto-RP and a BSR**

If there are only Cisco devices in your network (no routers from other vendors), there is no need to configure a BSR. Configure Auto-RP in a network that is running both PIMv1 and PIMv2.

If you have non-Cisco PIMv2 routers that need to interoperate with Cisco PIMv1 routers and multilayer switches, both Auto-RP and a BSR are required. We recommend that a Cisco PIMv2 router or multilayer switch be both the Auto-RP mapping agent and the BSR.

If you must have one or more BSRs, we have these recommendations:

- Configure the candidate BSRs as the RP-mapping agents for Auto-RP. For more information, see the “Configuring Auto-RP” section on page 45-25 and the “Configuring Candidate BSRs” section on page 45-31.

- For group prefixes advertised through Auto-RP, the PIMv2 BSR mechanism should not advertise a subrange of these group prefixes served by a different set of RPs. In a mixed PIMv1 and PIMv2 domain, have backup RPs serve the same group prefixes. This prevents the PIMv2 DRs from selecting a different RP from those PIMv1 DRs, due to the longest match lookup in the RP-mapping database.

Beginning in privileged EXEC mode, follow these steps to verify the consistency of group-to-RP mappings. This procedure is optional.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show ip pim rp [[group-name</td>
<td>group-address]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) For group-name, specify the name of the group about which to display RPs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) For group-address, specify the address of the group about which to display RPs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) Use the mapping keyword to display all group-to-RP mappings of which the Cisco device is aware (either configured or learned from Auto-RP).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show ip pim rp-hash group</td>
<td>On a PIMv2 router or multilayer switch, confirm that the same RP is the one that a PIMv1 system chooses.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For group, enter the group address for which to display RP information.</td>
</tr>
</tbody>
</table>
Monitoring the RP Mapping Information

To monitor the RP mapping information, use these commands in privileged EXEC mode:

- `show ip pim bsr` displays information about the elected BSR.
- `show ip pim rp-hash group` displays the RP that was selected for the specified group.
- `show ip pim rp [group-name | group-address | mapping]` displays how the switch learns of the RP (through the BSR or the Auto-RP mechanism).

Troubleshooting PIMv1 and PIMv2 Interoperability Problems

When debugging interoperability problems between PIMv1 and PIMv2, check these in the order shown:

1. Verify RP mapping with the `show ip pim rp-hash` privileged EXEC command, making sure that all systems agree on the same RP for the same group.
2. Verify interoperability between different versions of DRs and RPs. Make sure the RPs are interacting with the DRs properly (by responding with register-stops and forwarding decapsulated data packets from registers).

Configuring Advanced PIM Features

These sections describe the optional advanced PIM features:

- Understanding PIM Shared Tree and Source Tree, page 45-34
- Delaying the Use of PIM Shortest-Path Tree, page 45-36 (optional)
- Modifying the PIM Router-Query Message Interval, page 45-37 (optional)

Understanding PIM Shared Tree and Source Tree

By default, members of a group receive data from senders to the group across a single data-distribution tree rooted at the RP. Figure 45-6 shows this type of shared-distribution tree. Data from senders is delivered to the RP for distribution to group members joined to the shared tree.
If the data rate warrants, leaf routers (routers without any downstream connections) on the shared tree can use the data distribution tree rooted at the source. This type of distribution tree is called a shortest-path tree or source tree. By default, the software switches to a source tree upon receiving the first data packet from a source.

This process describes the move from a shared tree to a source tree:

1. A receiver joins a group; leaf Router C sends a join message toward the RP.
2. The RP puts a link to Router C in its outgoing interface list.
3. A source sends data; Router A encapsulates the data in a register message and sends it to the RP.
4. The RP forwards the data down the shared tree to Router C and sends a join message toward the source. At this point, data might arrive twice at Router C, once encapsulated and once natively.
5. When data arrives natively (unencapsulated) at the RP, it sends a register-stop message to Router A.
6. By default, reception of the first data packet prompts Router C to send a join message toward the source.
7. When Router C receives data on (S,G), it sends a prune message for the source up the shared tree.
8. The RP deletes the link to Router C from the outgoing interface of (S,G). The RP triggers a prune message toward the source.

Join and prune messages are sent for sources and RPs. They are sent hop-by-hop and are processed by each PIM device along the path to the source or RP. Register and register-stop messages are not sent hop-by-hop. They are sent by the designated router that is directly connected to a source and are received by the RP for the group.

Multiple sources sending to groups use the shared tree.

You can configure the PIM device to stay on the shared tree. For more information, see the “Delaying the Use of PIM Shortest-Path Tree” section on page 45-36.
Delaying the Use of PIM Shortest-Path Tree

The change from shared to source tree happens when the first data packet arrives at the last-hop router (Router C in Figure 45-6). This change occurs because the `ip pim spt-threshold` global configuration command controls that timing.

The shortest-path tree requires more memory than the shared tree but reduces delay. You might want to postpone its use. Instead of allowing the leaf router to immediately move to the shortest-path tree, you can specify that the traffic must first reach a threshold.

You can configure when a PIM leaf router should join the shortest-path tree for a specified group. If a source sends at a rate greater than or equal to the specified kbps rate, the multilayer switch triggers a PIM join message toward the source to construct a source tree (shortest-path tree). If the traffic rate from the source drops below the threshold value, the leaf router switches back to the shared tree and sends a prune message toward the source.

You can specify to which groups the shortest-path tree threshold applies by using a group list (a standard access list). If a value of 0 is specified or if the group list is not used, the threshold applies to all groups.

Beginning in privileged EXEC mode, follow these steps to configure a traffic rate threshold that must be reached before multicast routing is switched from the source tree to the shortest-path tree. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>access-list access-list-number {deny</td>
</tr>
<tr>
<td></td>
<td>Create a standard access list.</td>
</tr>
<tr>
<td></td>
<td>• For <code>access-list-number</code>, the range is 1 to 99.</td>
</tr>
<tr>
<td></td>
<td>• The <code>deny</code> keyword denies access if the conditions are matched.</td>
</tr>
<tr>
<td></td>
<td>• The <code>permit</code> keyword permits access if the conditions are matched.</td>
</tr>
<tr>
<td></td>
<td>• For <code>source</code>, specify the multicast group to which the threshold will apply.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) For <code>source-wildcard</code>, enter the wildcard bits in dotted decimal notation to be applied to the source. Place ones in the bit positions that you want to ignore.</td>
</tr>
<tr>
<td></td>
<td>Recall that the access list is always terminated by an implicit deny statement for everything.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>ip pim spt-threshold {kbps</td>
</tr>
<tr>
<td></td>
<td>Specify the threshold that must be reached before moving to shortest-path tree (spt).</td>
</tr>
<tr>
<td></td>
<td>• For <code>kbps</code>, specify the traffic rate in kbps. The default is 0.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Because of Catalyst 3750 Metro switch hardware limitations, 0 kbps is the only valid entry even though the range is 0 to 4294967.</td>
</tr>
<tr>
<td></td>
<td>• Specify <code>infinity</code> if you want all sources for the specified group to use the shared tree, never switching to the source tree.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) For <code>group-list access-list-number</code>, specify the access list created in Step 2. If the value is 0 or if the group-list is not used, the threshold applies to all groups.</td>
</tr>
</tbody>
</table>
Modifying the PIM Router-Query Message Interval

PIM routers and multilayer switches send PIM router-query messages to find which device will be the DR for each LAN segment (subnet). The DR is responsible for sending IGMP host-query messages to all hosts on the directly connected LAN.

With PIM DM operation, the DR has meaning only if IGMPv1 is in use. IGMPv1 does not have an IGMP querier election process, so the elected DR functions as the IGMP querier. With PIM SM operation, the DR is the device that is directly connected to the multicast source. It sends PIM register messages to notify the RP that multicast traffic from a source needs to be forwarded down the shared tree. In this case, the DR is the device with the highest IP address.

Beginning in privileged EXEC mode, follow these steps to modify the router-query message interval. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>ip pim query-interval seconds</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
</tr>
<tr>
<td>Step 5</td>
<td>show ip igmp interface [interface-id]</td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To return to the default setting, use the `no ip pim query-interval [seconds]` interface configuration command.
Configuring Optional IGMP Features

These sections describe how to configure optional IGMP features:

- Default IGMP Configuration, page 45-38
- Configuring the Switch as a Member of a Group, page 45-38 (optional)
- Controlling Access to IP Multicast Groups, page 45-39 (optional)
- Changing the IGMP Version, page 45-40 (optional)
- Modifying the IGMP Host-Query Message Interval, page 45-41 (optional)
- Changing the IGMP Query Timeout for IGMPv2, page 45-42 (optional)
- Changing the Maximum Query Response Time for IGMPv2, page 45-42 (optional)
- Configuring the Switch as a Statically Connected Member, page 45-43 (optional)

Default IGMP Configuration

Table 45-4 shows the default IGMP configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multilayer switch as a member of a multicast group</td>
<td>No group memberships are defined.</td>
</tr>
<tr>
<td>Access to multicast groups</td>
<td>All groups are allowed on an interface.</td>
</tr>
<tr>
<td>IGMP version</td>
<td>Version 2 on all interfaces.</td>
</tr>
<tr>
<td>IGMP host-query message interval</td>
<td>60 seconds on all interfaces.</td>
</tr>
<tr>
<td>IGMP query timeout</td>
<td>60 seconds on all interfaces.</td>
</tr>
<tr>
<td>IGMP maximum query response time</td>
<td>10 seconds on all interfaces.</td>
</tr>
<tr>
<td>Multilayer switch as a statically connected member</td>
<td>Disabled.</td>
</tr>
</tbody>
</table>

Configuring the Switch as a Member of a Group

You can configure the switch as a member of a multicast group and discover multicast reachability in a network. If all the multicast-capable routers and multilayer switches that you administer are members of a multicast group, pinging that group causes all these devices to respond. The devices respond to ICMP echo-request packets addressed to a group of which they are members. Another example is the multicast trace-route tools provided in the software.

Caution

Performing this procedure might impact the CPU performance because the CPU will receive all data traffic for the group address.
Beginning in privileged EXEC mode, follow these steps to configure the switch to be a member of a group. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>ip igmp join-group group-address</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>show ip igmp interface [interface-id]</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To cancel membership in a group, use the no ip igmp join-group group-address interface configuration command.

This example shows how to enable the switch to join multicast group 255.2.2.2:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip igmp join-group 255.2.2.2
```

### Controlling Access to IP Multicast Groups

The switch sends IGMP host-query messages to find which multicast groups have members on attached local networks. The switch then forwards to these group members all packets addressed to the multicast group. You can place a filter on each interface to restrict the multicast groups that hosts on the subnet serviced by the interface can join.

Beginning in privileged EXEC mode, follow these steps to filter multicast groups allowed on an interface. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>ip igmp access-group access-list-number</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>exit</td>
</tr>
</tbody>
</table>
To disable groups on an interface, use the **no ip igmp access-group** interface configuration command.

This example shows how to configure hosts attached to a port as able to join only group 255.2.2.2:

```
Switch(config)# access-list 1 255.2.2.2 0.0.0.0
Switch(config-if)# interface gigabitethernet1/0/1
Switch(config-if)# ip igmp access-group 1
```

### Changing the IGMP Version

By default, the switch uses IGMP Version 2, which provides features such as the IGMP query timeout and the maximum query response time.

All systems on the subnet must support the same version. The switch does not automatically detect Version 1 systems and switch to Version 1. You can mix Version 1 and Version 2 hosts on the subnet because Version 2 routers or switches always work correctly with IGMPv1 hosts.

Configure the switch for Version 1 if your hosts do not support Version 2.

Beginning in privileged EXEC mode, follow these steps to change the IGMP version. This procedure is optional.

```
Step 1 configure terminal
Step 2 interface interface-id
Step 3 ip igmp version {1 | 2}
Step 4 end
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><code>interface interface-id</code></td>
<td>Specify the interface to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>`ip igmp version {1</td>
<td>2}`</td>
</tr>
<tr>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
Modifying the IGMP Host-Query Message Interval

The switch periodically sends IGMP host-query messages to discover which multicast groups are present on attached networks. These messages are sent to the all-hosts multicast group (224.0.0.1) with a time-to-live (TTL) of 1. The switch sends host-query messages to refresh its knowledge of memberships present on the network. If, after some number of queries, the software discovers that no local hosts are members of a multicast group, the software stops forwarding multicast packets to the local network from remote origins for that group and sends a prune message upstream toward the source.

The switch elects a PIM designated router (DR) for the LAN (subnet). The DR is the router or multilayer switch with the highest IP address for IGMPv2. For IGMPv1, the DR is elected according to the multicast routing protocol that runs on the LAN. The designated router is responsible for sending IGMP host-query messages to all hosts on the LAN. In sparse mode, the designated router also sends PIM register and PIM join messages toward the RP router.

Beginning in privileged EXEC mode, follow these steps to modify the host-query interval. This procedure is optional.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>interface interface-id</td>
<td>Specify the interface to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>3</td>
<td>ip igmp query-interval seconds</td>
<td>Configure the frequency at which the designated router sends IGMP host-query messages. By default, the designated router sends IGMP host-query messages every 60 seconds to keep the IGMP overhead very low on hosts and networks. The range is 1 to 65535.</td>
</tr>
<tr>
<td>4</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>5</td>
<td>show ip igmp interface [interface-id]</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>6</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default setting, use the **no ip igmp version** interface configuration command.
Changing the IGMP Query Timeout for IGMPv2

If you are using IGMPv2, you can specify the period of time before the switch takes over as the querier for the interface. By default, the switch waits twice the query interval controlled by the `ip igmp query-interval` interface configuration command. After that time, if the switch has received no queries, it becomes the querier.

You can configure the query interval by entering the `show ip igmp interface interface-id` privileged EXEC command.

Beginning in privileged EXEC mode, follow these steps to change the IGMP query timeout. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>ip igmp querier-timeout seconds</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
</tr>
<tr>
<td>Step 5</td>
<td>show ip igmp interface [interface-id]</td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To return to the default setting, use the `no ip igmp querier-timeout` interface configuration command.

Changing the Maximum Query Response Time for IGMPv2

If you are using IGMPv2, you can change the maximum query response time advertised in IGMP queries. The maximum query response time enables the switch to quickly detect that there are no more directly connected group members on a LAN. Decreasing the value enables the switch to prune groups faster.

Beginning in privileged EXEC mode, follow these steps to change the maximum query response time. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>ip igmp query-max-response-time seconds</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
</tr>
<tr>
<td>Step 5</td>
<td>show ip igmp interface [interface-id]</td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>
To return to the default setting, use the `no ip igmp query-max-response-time` interface configuration command.

### Configuring the Switch as a Statically Connected Member

Sometimes there is either no group member on a network segment or a host cannot report its group membership by using IGMP. However, you might want multicast traffic to go to that network segment. These are ways to pull multicast traffic down to a network segment:

- Use the `ip igmp join-group` interface configuration command. With this method, the switch accepts the multicast packets in addition to forwarding them. Accepting the multicast packets prevents the switch from fast switching.

- Use the `ip igmp static-group` interface configuration command. With this method, the switch does not accept the packets itself, but only forwards them. This method enables fast switching. The outgoing interface appears in the IGMP cache, but the switch itself is not a member, as evidenced by lack of an `L` (local) flag in the multicast route entry.

Beginning in privileged EXEC mode, follow these steps to configure the switch itself to be a statically connected member of a group (and enable fast switching). This procedure is optional.

**Command Purpose**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>interface interface-id</code></td>
<td>Specify the interface to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>ip igmp static-group group-address</code></td>
<td>Configure the switch as a statically connected member of a group. By default, this feature is disabled.</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>show ip igmp interface [interface-id]</code></td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 6</td>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To remove the switch as a member of the group, use the `no ip igmp static-group group-address` interface configuration command.

### Configuring Optional Multicast Routing Features

This section describes how to configure optional multicast routing features, which are grouped as follows:

- Features for Layer 2 connectivity and MBONE multimedia conference session and set up:
  - Enabling CGMP Server Support, page 45-44 (optional)
  - Configuring sdr Listener Support, page 45-45 (optional)

- Features that control bandwidth utilization:
  - Configuring an IP Multicast Boundary, page 45-46 (optional)

- Procedure for configuring a multicast within a VPN routing/forwarding (VRF) table:
  - Configuring Multicast VRFs, page 36-92 (optional)
Enabling CGMP Server Support

The switch serves as a CGMP server for devices that do not support IGMP snooping but have CGMP client functionality. CGMP is a protocol used on Cisco routers and multilayer switches connected to Layer 2 Catalyst switches to perform tasks similar to those performed by IGMP. CGMP is necessary because the Layer 2 switch cannot distinguish between IP multicast data packets and IGMP report messages, which are both at the MAC-level and are addressed to the same group address.

Beginning in privileged EXEC mode, follow these steps to enable the CGMP server on the switch interface. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Specify the interface that is connected to the Layer 2 Catalyst switch, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3 ip cgmp [proxy]</td>
<td>Enable CGMP on the interface. By default, CGMP is disabled on all interfaces. Enabling CGMP triggers a CGMP join message. Enable CGMP only on Layer 3 interfaces connected to Layer 2 Catalyst switches. (Optional) When you enter the proxy keyword, the CGMP proxy function is enabled. The proxy router advertises the existence of non-CGMP-capable routers by sending a CGMP join message with the non-CGMP-capable router MAC address and a group address of 0000.0000.0000.</td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5 show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 6 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Verify the Layer 2 Catalyst switch CGMP-client configuration. For more information, see the documentation that shipped with the product.</td>
</tr>
</tbody>
</table>

To disable CGMP on the interface, use the no ip cgmp interface configuration command.

When multiple Cisco CGMP-capable devices are connected to a switched network and the ip cgmp proxy command is needed, we recommend that all devices be configured with the same CGMP option and have precedence for becoming the IGMP querier over non-Cisco routers.
Configuring sdr Listener Support

The MBONE is the small subset of Internet routers and hosts that are interconnected and capable of forwarding IP multicast traffic. Other interesting multimedia content is often broadcast over the MBONE. Before you can join a multimedia session, you need to know what multicast group address and interface are being used for the session, when the session is going to be active, and what sort of applications (audio, video, and so forth) are required on your workstation. The MBONE Session Directory version 2 (sdr) tool provides this information. This freeware application can be downloaded from several sites on the World Wide Web, one of which is http://www.video.ja.net/mice/index.html.

SDR is a multicast application that listens to a well-known multicast group address and interface for Session Announcement Protocol (SAP) multicast packets from SAP clients, which announce their conference sessions. These SAP packets contain a session description, the time the session is active, its IP multicast group addresses, media format, contact person, and other information about the advertised multimedia session. The information in the SAP packet appears in the SDR Session Announcement window.

Enabling sdr Listener Support

By default, the switch does not listen to session directory advertisements.

Beginning in privileged EXEC mode, follow these steps to enable the switch to join the default session directory group (224.2.127.254) on the interface and listen to session directory advertisements. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
<tr>
<td></td>
<td>Specify the interface to be enabled for sdr,</td>
</tr>
<tr>
<td></td>
<td>and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>ip sdr listen</td>
</tr>
<tr>
<td></td>
<td>Enable sdr listener support.</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
</tr>
<tr>
<td></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5</td>
<td>show running-config</td>
</tr>
<tr>
<td></td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</td>
</tr>
<tr>
<td></td>
<td>(Optional) Save your entries in the</td>
</tr>
<tr>
<td></td>
<td>configuration file.</td>
</tr>
</tbody>
</table>

To disable sdr support, use the **no ip sdr listen** interface configuration command.

Limiting How Long an sdr Cache Entry Exists

By default, entries are never deleted from the sdr cache. You can limit how long the entry remains active so that if a source stops advertising SAP information, old advertisements are not needlessly kept.

Beginning in privileged EXEC mode, follow these steps to limit how long an sdr cache entry stays active in the cache. This procedure is optional.
### Configuring Optional Multicast Routing Features

#### Configuring Optional Multicast Routing Features

To return to the default setting, use the `no ip sdr cache-timeout` global configuration command. To delete the entire cache, use the `clear ip sdr` privileged EXEC command.

To display the session directory cache, use the `show ip sdr` privileged EXEC command.

#### Configuring an IP Multicast Boundary

Administratively-scoped boundaries can be used to limit the forwarding of multicast traffic outside of a domain or subdomain. This approach uses a special range of multicast addresses, called *administratively-scoped addresses*, as the boundary mechanism. If you configure an administratively-scoped boundary on a routed port, multicast traffic whose multicast group addresses fall in this range can not enter or exit this port, thereby providing a firewall for multicast traffic in this address range.

**Note**
Multicast boundaries and TTL thresholds control the scoping of multicast domains; however, TTL thresholds are not supported by the switch. You should use multicast boundaries instead of TTL thresholds to limit the forwarding of multicast traffic outside of a domain or a subdomain.

Figure 45-7 shows that Company XYZ has an administratively-scoped boundary set for the multicast address range 239.0.0.0/8 on all routed ports at the perimeter of its network. This boundary prevents any multicast traffic in the range 239.0.0.0 through 239.255.255.255 from entering or leaving the network. Similarly, the engineering and marketing departments have an administratively-scoped boundary of 239.128.0.0/16 around the perimeter of their networks. This boundary prevents multicast traffic in the range of 239.128.0.0 through 239.128.255.255 from entering or leaving their respective networks.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> ip sdr cache-timeout minutes</td>
<td>Limit how long an sdr cache entry stays active in the cache. By default, entries are never deleted from the cache. For minutes, the range is 1 to 4294967295.</td>
</tr>
<tr>
<td><strong>Step 3</strong> end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong> show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td><strong>Step 5</strong> copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
You can define an administratively-scoped boundary on a routed port for multicast group addresses. A standard access list defines the range of addresses affected. When a boundary is defined, no multicast data packets are allowed to flow across the boundary from either direction. The boundary allows the same multicast group address to be reused in different administrative domains.

The IANA has designated the multicast address range 239.0.0.0 to 239.255.255 as the administratively-scoped addresses. This range of addresses can then be reused in domains administered by different organizations. The addresses would be considered local, not globally unique.

Beginning in privileged EXEC mode, follow these steps to set up an administratively-scoped boundary. This procedure is optional.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>access-list access-list-number [deny</td>
<td>Create a standard access list, repeating the command as many times as necessary.</td>
</tr>
<tr>
<td></td>
<td>permit] source [source-wildcard]</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For access-list-number, the range is 1 to 99.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The deny keyword denies access if the conditions are matched. The permit keyword permits access if the conditions are matched.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For source, enter the number of the network or host from which the packet is being sent.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) For source-wildcard, enter the wildcard bits in dotted decimal notation to be applied to the source. Place ones in the bit positions that you want to ignore.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Recall that the access list is always terminated by an implicit deny statement for everything.</td>
</tr>
<tr>
<td>3</td>
<td>interface interface-id</td>
<td>Specify the interface to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>4</td>
<td>ip multicast boundary access-list-number</td>
<td>Configure the boundary, specifying the access list you created in Step 2.</td>
</tr>
<tr>
<td>5</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>6</td>
<td>show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>7</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
To remove the boundary, use the **no ip multicast boundary** interface configuration command. This example shows how to set up a boundary for all administratively-scoped addresses:

Switch(config)# access-list 1 deny 239.0.0.0 0.255.255.255
Switch(config)# access-list 1 permit 224.0.0.0 15.255.255.255
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip multicast boundary 1

## Configuring Basic DVMRP Interoperability Features

These sections describe how to perform basic configuration tasks on your switch to interoperate with DVMRP devices:

- Configuring DVMRP Interoperability, page 45-48 (optional)
- Configuring a DVMRP Tunnel, page 45-50 (optional)
- Advertising Network 0.0.0.0 to DVMRP Neighbors, page 45-52 (optional)
- Responding to mrinfo Requests, page 45-53 (optional)

For more advanced DVMRP features, see the “Configuring Advanced DVMRP Interoperability Features” section on page 45-53.

## Configuring DVMRP Interoperability

Cisco multicast routers and multilayer switches using PIM can interoperate with non-Cisco multicast routers that use the DVMRP. PIM devices dynamically discover DVMRP multicast routers on attached networks by listening to DVMR probe messages. When a DVMRP neighbor has been discovered, the PIM device periodically sends DVMRP report messages advertising the unicast sources reachable in the PIM domain. By default, directly connected subnets and networks are advertised. The device forwards multicast packets that have been forwarded by DVMRP routers and, in turn, forwards multicast packets to DVMRP routers.

You can configure an access list on the PIM routed port connected to the MBONE to limit the number of unicast routes that are advertised in DVMRP route reports. Otherwise, all routes in the unicast routing table are advertised.

The **mrouted protocol** is a public-domain implementation of DVMRP. You must use mrouted Version 3.8 (which implements a nonpruning version of DVMRP) when Cisco routers and multilayer switches are directly connected to DVMRP routers or interoperate with DVMRP routers over an MBONE tunnel. DVMRP advertisements produced by the Cisco IOS software can cause older versions of the mrouted protocol to corrupt their routing tables and those of their neighbors.

You can configure what sources are advertised and what metrics are used by configuring the **ip dvmrp metric** interface configuration command. You can also direct all sources learned through a particular unicast routing process to be advertised into DVMRP.
Beginning in privileged EXEC mode, follow these steps to configure the sources that are advertised and the metrics that are used when DVMRP route-report messages are sent. This procedure is optional.

### Command Purpose

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>access-list access-list-number {deny</td>
<td>permit} source [source-wildcard]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- For access-list-number, the range is 1 to 99.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- The deny keyword denies access if the conditions are matched. The permit keyword permits access if the conditions are matched.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- For source, enter the number of the network or host from which the packet is being sent.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- (Optional) For source-wildcard, enter the wildcard bits in dotted decimal notation to be applied to the source. Place ones in the bit positions that you want to ignore.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Recall that the access list is always terminated by an implicit deny statement for everything.</td>
</tr>
<tr>
<td>3</td>
<td>interface interface-id</td>
<td>Specify the interface connected to the MBONE and enabled for multicast routing, and enter interface configuration mode.</td>
</tr>
<tr>
<td>4</td>
<td>ip dvmrp metric metric [list access-list-number] [[protocol process-id]</td>
<td>Configure the metric associated with a set of destinations for DVMRP reports.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- For metric, the range is 0 to 32. A value of 0 means that the route is not advertised. A value of 32 is equivalent to infinity (unreachable).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- (Optional) For list access-list-number, enter the access list number created in Step 2. If specified, only the multicast destinations that match the access list are reported with the configured metric.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- (Optional) For protocol process-id, enter the name of the unicast routing protocol, such as eigrp, igrp, ospf, rip, static, or dvmrp, and the process ID number of the routing protocol. If specified, only routes learned by the specified routing protocol are advertised in DVMRP report messages.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- (Optional) If specified, the dvmrp keyword allows routes from the DVMRP routing table to be advertised with the configured metric or filtered.</td>
</tr>
<tr>
<td>5</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>6</td>
<td>show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>7</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable the metric or route map, use the `no ip dvmrp metric metric [list access-list-number] [[protocol process-id] | [dvmrp]]` or the `no ip dvmrp metric metric route-map map-name` interface configuration command.

A more sophisticated way to achieve the same results as the preceding command is to use a route map (ip dvmrp metric metric route-map map-name interface configuration command) instead of an access list. You subject unicast routes to route-map conditions before they are injected into DVMRP.
This example shows how to configure DVMRP interoperability when the PIM device and the DVMRP router are on the same network segment. In this example, access list 1 advertises the networks (198.92.35.0, 198.92.36.0, 198.92.37.0, 131.108.0.0, and 150.136.0.0) to the DVMRP router, and access list 2 prevents all other networks from being advertised (ip dvmrp metric 0 interface configuration command).

Switch(config-if)# interface gigabitethernet1/0/1
Switch(config-if)# ip address 131.119.244.244 255.255.255.0
Switch(config-if)# ip pim dense-mode
Switch(config-if)# ip dvmrp metric 1 list 1
Switch(config-if)# ip dvmrp metric 0 list 2
Switch(config-if)# exit
Switch(config)# access-list 1 permit 198.92.35.0 0.0.0.255
Switch(config)# access-list 1 permit 198.92.36.0 0.0.0.255
Switch(config)# access-list 1 permit 198.92.37.0 0.0.0.255
Switch(config)# access-list 1 permit 131.108.0.0 0.0.255.255
Switch(config)# access-list 1 permit 150.136.0.0 0.0.255.255
Switch(config)# access-list 1 deny 0.0.0.0 255.255.255.255
Switch(config)# access-list 2 permit 0.0.0.0 255.255.255.255

### Configuring a DVMRP Tunnel

The software supports DVMRP tunnels to the MBONE. You can configure a DVMRP tunnel on a router or multilayer switch if the other end is running DVMRP. The software then sends and receives multicast packets through the tunnel. This strategy enables a PIM domain to connect to the DVMRP router when all routers on the path do not support multicast routing. You cannot configure a DVMRP tunnel between two routers.

When a Cisco router or multilayer switch runs DVMRP through a tunnel, it advertises sources in DVMRP report messages, much as it does on real networks. The software also caches DVMRP report messages it receives and uses them in its RPF calculation. This behavior enables the software to forward multicast packets received through the tunnel.

When you configure a DVMRP tunnel, you should assign an IP address to a tunnel in these cases:

- To send IP packets through the tunnel
- To configure the software to perform DVMRP summarization

The software does not advertise subnets through the tunnel if the tunnel has a different network number from the subnet. In this case, the software advertises only the network number through the tunnel.

Beginning in privileged EXEC mode, follow these steps to configure a DVMRP tunnel. This procedure is optional.
<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
</tbody>
</table>
| **Step 2** | access-list access-list-number {deny | permit} source [source-wildcard] | Create a standard access list, repeating the command as many times as necessary.  
- For access-list-number, the range is 1 to 99.  
- The deny keyword denies access if the conditions are matched. The permit keyword permits access if the conditions are matched.  
- For source, enter the number of the network or host from which the packet is being sent.  
- (Optional) For source-wildcard, enter the wildcard bits in dotted decimal notation to be applied to the source. Place ones in the bit positions that you want to ignore.  
Recall that the access list is always terminated by an implicit deny statement for everything. |
| **Step 3** | interface tunnel number | Specify a tunnel port, and enter interface configuration mode. |
| **Step 4** | tunnel source ip-address | Specify the source address of the tunnel port. Enter the IP address of the interface on the switch. |
| **Step 5** | tunnel destination ip-address | Specify the destination address of the tunnel port. Enter the IP address of the mrouted router. |
| **Step 6** | tunnel mode dvmrp | Configure the encapsulation mode for the tunnel to DVMRP. |
| **Step 7** | ip address address mask  
or  
ip unnumbered type number | Assign an IP address to the interface.  
or  
Configure the interface as unnumbered. |
| **Step 8** | ip pim [dense-mode | sparse-mode] | Configure the PIM mode on the interface. |
| **Step 9** | ip dvmrp accept-filter access-list-number [distance] neighbor-list access-list-number | Configure an acceptance filter for incoming DVMRP reports.  
By default, all destination reports are accepted with a distance of 0. Reports from all neighbors are accepted.  
- For access-list-number, specify the access list number created in Step 2. Any sources that match the access list are stored in the DVMRP routing table with distance.  
- (Optional) For distance, enter the administrative distance to the destination. By default, the administrative distance for DVMRP routes is 0 and take precedence over unicast routing table routes. If you have two paths to a source, one through unicast routing (using PIM as the multicast routing protocol) and another using DVMRP, and if you want to use the PIM path, increase the administrative distance for DVMRP routes. The range is 1 to 255.  
- For neighbor-list access-list-number, enter the number of the neighbor list created in Step 2. DVMRP reports are accepted only by those neighbors on the list. |
| **Step 10** | end | Return to privileged EXEC mode. |
To disable the filter, use the `no ip dvmrp accept-filter access-list-number [distance] neighbor-list` interface configuration command.

This example shows how to configure a DVMRP tunnel. In this configuration, the IP address of the tunnel on the Cisco switch is assigned `unnumbered`, which causes the tunnel to appear to have the same IP address as port 1. The tunnel endpoint source address is 172.16.2.1, and the tunnel endpoint address of the remote DVMRP router to which the tunnel is connected is 192.168.1.10. Any packets sent through the tunnel are encapsulated in an outer IP header. The Cisco switch is configured to accept incoming DVMRP reports with a distance of 100 from 198.92.37.0 through 198.92.37.255.

```
Switch(config)# ip multicast-routing
Switch(config)# interface tunnel 0
Switch(config-if)# ip unnumbered gigabitethernet1/0/1
Switch(config-if)# ip pim dense-mode
Switch(config-if)# tunnel source gigabitethernet1/0/1
Switch(config-if)# tunnel destination 192.168.1.10
Switch(config-if)# tunnel mode dvmrp
Switch(config-if)# ip dvmrp accept-filter 1 100
Switch(config-if)# interface gigabitethernet1/0/1
Switch(config-if)# ip address 172.16.2.1 255.255.255.0
Switch(config-if)# ip pim dense-mode
Switch(config)# exit
Switch(config)# access-list 1 permit 198.92.37.0 0.0.0.255
```

**Advertising Network 0.0.0.0 to DVMRP Neighbors**

If your switch is a neighbor of an mrouted version 3.6 device, you can configure the software to advertise network 0.0.0.0 (the default route) to the DVMRP neighbor. The DVMRP default route computes the RPF information for any multicast sources that do not match a more specific route.

Do not advertise the DVMRP default into the MBONE.

Beginning in privileged EXEC mode, follow these steps to advertise network 0.0.0.0 to DVMRP neighbors on an interface. This procedure is optional.

```
Step 1
configure terminal
Enter global configuration mode.

Step 2
interface interface-id
Specify the interface that is connected to the DVMRP router, and enter interface configuration mode.

Step 3
ip dvmrp default-information {originated | only}
Advertise network 0.0.0.0 to DVMRP neighbors.
Use this command only when the switch is a neighbor of mrouted version 3.6 machines.
The keywords have these meanings:
- `originated`—Specifies that other routes more specific than 0.0.0.0 can also be advertised.
- `only`—Specifies that no DVMRP routes other than 0.0.0.0 are advertised.
```
To prevent the default route advertisement, use the `no ip dvmrp default-information` interface configuration command.

### Responding to mrinfo Requests

The software answers mrinfo requests sent by mrouted systems and Cisco routers and multilayer switches. The software returns information about neighbors through DVMRP tunnels and all the routed ports. This information includes the metric (always set to 1), the configured TTL threshold, the status of the port, and various flags. You can also use the `mrinfo` privileged EXEC command to query the router or switch itself, as in this example:

```
Switch# mrinfo
171.69.214.27 (mm1-7kd.cisco.com) [version cisco 11.1] [flags: PMS]:
171.69.214.27 -> 171.69.214.26 (mm1-r7kb.cisco.com) [1/0/pim/querier]
171.69.214.27 -> 171.69.214.25 (mm1-45a.cisco.com) [1/0/pim/querier]
171.69.214.33 -> 171.69.214.34 (mm1-45c.cisco.com) [1/0/pim]
171.69.214.137 -> 0.0.0.0 [1/0/pim/querier/down/leaf]
171.69.214.203 -> 0.0.0.0 [1/0/pim/querier/down/leaf]
171.69.214.18 -> 171.69.214.20 (mm1-45e.cisco.com) [1/0/pim]
171.69.214.18 -> 171.69.214.19 (mm1-45c.cisco.com) [1/0/pim]
171.69.214.18 -> 171.69.214.17 (mm1-45a.cisco.com) [1/0/pim]
```

### Configuring Advanced DVMRP Interoperability Features

Cisco routers and multilayer switches run PIM to forward multicast packets to receivers and receive multicast packets from senders. It is also possible to propagate DVMRP routes into and through a PIM cloud. PIM uses this information; however, Cisco routers and multilayer switches do not implement DVMRP to forward multicast packets.

These sections describe how to perform advanced optional configuration tasks on your switch to interoperate with DVMRP devices:

- **Enabling DVMRP Unicast Routing, page 45-54** (optional)
- **Rejecting a DVMRP Nonpruning Neighbor, page 45-54** (optional)
- **Controlling Route Exchanges, page 45-57** (optional)

For information on basic DVMRP features, see the “Configuring Basic DVMRP Interoperability Features” section on page 45-48.
Enabling DVMRP Unicast Routing

Because multicast routing and unicast routing require separate topologies, PIM must follow the multicast topology to build loopless distribution trees. Using DVMRP unicast routing, Cisco routers, multilayer switches, and mrouted-based machines exchange DVMRP unicast routes, to which PIM can then reverse-path forward.

Cisco devices do not perform DVMRP multicast routing among each other, but they can exchange DVMRP routes. The DVMRP routes provide a multicast topology that might differ from the unicast topology. This enables PIM to run over the multicast topology, thereby enabling sparse-mode PIM over the MBONE topology.

When DVMRP unicast routing is enabled, the router or switch caches routes learned in DVMRP report messages in a DVMRP routing table. When PIM is running, these routes might be preferred over routes in the unicast routing table, enabling PIM to run on the MBONE topology when it is different from the unicast topology.

DVMRP unicast routing can run on all interfaces. For DVMRP tunnels, it uses DVMRP multicast routing. This feature does not enable DVMRP multicast routing among Cisco routers and multilayer switches. However, if there is a DVMRP-capable multicast router, the Cisco device can do PIM/DVMRP multicast routing.

Beginning in privileged EXEC mode, follow these steps to enable DVMRP unicast routing. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Specify the interface that is connected to the DVMRP router, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3 ip dvmrp unicast-routing</td>
<td>Enable DVMRP unicast routing (to send and receive DVMRP routes). This feature is disabled by default.</td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5 show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 6 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable this feature, use the `no ip dvmrp unicast-routing` interface configuration command.

Rejecting a DVMRP Nonpruning Neighbor

By default, Cisco devices accept all DVMRP neighbors as peers, regardless of their DVMRP capability. However, some non-Cisco devices run old versions of DVMRP that cannot prune, so they continuously receive forwarded packets, wasting bandwidth. Figure 45-8 shows this scenario.
You can prevent the switch from peering (communicating) with a DVMRP neighbor if that neighbor does not support DVMRP pruning or grafting. To do so, configure the switch (which is a neighbor to the leaf, nonpruning DVMRP machine) with the `ip dvmrp reject-non-pruners` interface configuration command on the interface connected to the nonpruning machine as shown in Figure 45-9. In this case, when the switch receives DVMRP probe or report message without the prune-capable flag set, the switch logs a syslog message and discards the message.
Configuring Advanced DVMRP Interoperability Features

Chapter 45 Configuring IP Multicast Routing

Figure 45-9 Router Rejects Nonpruning DVMRP Neighbor

Note that the `ip dvmrp reject-non-pruners` interface configuration command prevents peering with neighbors only. If there are any nonpruning routers multiple hops away (downstream toward potential receivers) that are not rejected, a nonpruning DVMRP network might still exist.

Beginning in privileged EXEC mode, follow these steps to prevent peering with nonpruning DVMRP neighbors. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1  <code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2  <code>interface interface-id</code></td>
<td>Specify the interface connected to the nonpruning DVMRP neighbor, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3  <code>ip dvmrp reject-non-pruners</code></td>
<td>Prevent peering with nonpruning DVMRP neighbors.</td>
</tr>
<tr>
<td>Step 4  <code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5  <code>show running-config</code></td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 6  <code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable this function, use the `no ip dvmrp reject-non-pruners` interface configuration command.
Controlling Route Exchanges

These sections describe how to tune the Cisco device advertisements of DVMRP routes:

- Limiting the Number of DVMRP Routes Advertised, page 45-57 (optional)
- Changing the DVMRP Route Threshold, page 45-57 (optional)
- Configuring a DVMRP Summary Address, page 45-58 (optional)
- Disabling DVMRP Autosummarization, page 45-60 (optional)
- Adding a Metric Offset to the DVMRP Route, page 45-60 (optional)

Limiting the Number of DVMRP Routes Advertised

By default, only 7000 DVMRP routes are advertised over an interface enabled to run DVMRP (that is, a DVMRP tunnel, an interface where a DVMRP neighbor has been discovered, or an interface configured to run the `ip dvmrp unicast-routing` interface configuration command).

Beginning in privileged EXEC mode, follow these steps to change the DVMRP route limit. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 ip dvmrp route-limit <code>count</code></td>
<td>Change the number of DVMRP routes advertised over an interface enabled for DVMRP. This command prevents misconfigured <code>ip dvmrp metric</code> interface configuration commands from causing massive route injection into the MBONE. By default, 7000 routes are advertised. The range is 0 to 4294967295.</td>
</tr>
<tr>
<td>Step 3 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4 show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 5 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To configure no route limit, use the `no ip dvmrp route-limit` global configuration command.

Changing the DVMRP Route Threshold

By default, 10,000 DVMRP routes can be received per interface within a 1-minute interval. When that rate is exceeded, a syslog message is issued, warning that there might be a route surge occurring. The warning is typically used to quickly detect when devices have been misconfigured to inject a large number of routes into the MBONE.
Beginning in privileged EXEC mode, follow these steps to change the threshold number of routes that trigger the warning. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 ip dvmrp routehog-notification</td>
<td>Configure the number of routes that trigger a syslog message.</td>
</tr>
<tr>
<td>route-count</td>
<td>The default is 10,000 routes. The range is 1 to 4294967295.</td>
</tr>
<tr>
<td>Step 3 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4 show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 5 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default setting use the **no ip dvmrp routehog-notification** global configuration command.

Use the **show ip igmp interface** privileged EXEC command to display a running count of routes. When the count is exceeded, ***ALERT*** is appended to the line.

### Configuring a DVMRP Summary Address

By default, a Cisco device advertises in DVMRP route-report messages only connected unicast routes (that is, only routes to subnets that are directly connected to the router) from its unicast routing table. These routes undergo normal DVMRP classful route summarization. This process depends on whether the route being advertised is in the same classful network as the interface over which it is being advertised.

**Figure 45-10** shows an example of the default behavior. This example shows that the DVMRP report sent by the Cisco router contains the three original routes received from the DVMRP router that have been poison-reversed by adding 32 to the DVMRP metric. Listed after these routes are two routes that are advertisements for the two directly connected networks (176.32.10.0/24 and 176.32.15.0/24) that were taken from the unicast routing table. Because the DVMRP tunnel shares the same IP address as Fast Ethernet port 1 and falls into the same Class B network as the two directly connected subnets, classful summarization of these routes was not performed. As a result, the DVMRP router is able to poison-reverse only these two routes to the directly connected subnets and is able to only RPF properly for multicast traffic sent by sources on these two Ethernet segments. Any other multicast source in the network behind the Cisco router that is not on these two Ethernet segments does not properly RPF-check on the DVMRP router and is discarded.

You can force the Cisco router to advertise the summary address (specified by the address and mask pair in the **ip dvmrp summary-address address mask** interface configuration command) in place of any route that falls in this address range. The summary address is sent in a DVMRP route report if the unicast routing table contains at least one route in this range; otherwise, the summary address is not advertised. In **Figure 45-10**, you configure the **ip dvmrp summary-address** command on the Cisco router tunnel port. As a result, the Cisco router sends only a single summarized Class B advertisement for network 176.32.0.0.16 from the unicast routing table.
Beginning in privileged EXEC mode, follow these steps to customize the summarization of DVMRP routes if the default classful autosummarization does not suit your needs. This procedure is optional.

**Note** At least one more-specific route must be present in the unicast routing table before a configured summary address is advertised.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>ip dvmrp summary-address address mask [metric value]</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
</tr>
<tr>
<td>Step 5</td>
<td>show running-config</td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To remove the summary address, use the `no ip dvmrp summary-address address mask [metric value]` interface configuration command.
Disabling DVMRP Autosummarization

By default, the software automatically performs some level of DVMRP summarization. Disable this function if you want to advertise all routes, not just a summary. In some special cases, you can use the neighboring DVMRP router with all subnet information to better control the flow of multicast traffic in the DVMRP network. One such case might occur if the PIM network is connected to the DVMRP cloud at several points and more specific (unsummarized) routes are being injected into the DVMRP network to advertise better paths to individual subnets inside the PIM cloud.

If you configure the `ip dvmrp summary-address` interface configuration command and did not configure `no ip dvmrp auto-summary`, you get both custom and autosummaries.

Beginning in privileged EXEC mode, follow these steps to disable DVMRP autosummarization. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: <code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2: <code>interface interface-id</code></td>
<td>Specify the interface connected to the DVMRP router, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3: <code>no ip dvmrp auto-summary</code></td>
<td>Disable DVMRP autosummarization.</td>
</tr>
<tr>
<td>Step 4: <code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5: <code>show running-config</code></td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 6: <code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To re-enable auto summarization, use the `ip dvmrp auto-summary` interface configuration command.

Adding a Metric Offset to the DVMRP Route

By default, the switch increments by one the metric (hop count) of a DVMRP route advertised in incoming DVMRP reports. You can change the metric if you want to favor or not favor a certain route.

For example, a route is learned by multilayer switch A, and the same route is learned by multilayer switch B with a higher metric. If you want to use the path through switch B because it is a faster path, you can apply a metric offset to the route learned by switch A to make it larger than the metric learned by switch B, and you can choose the path through switch B.

Beginning in privileged EXEC mode, follow these steps to change the default metric. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: <code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2: <code>interface interface-id</code></td>
<td>Specify the interface to be configured, and enter interface configuration mode.</td>
</tr>
</tbody>
</table>
To return to the default setting, use the `no ip dvmrp metric-offset` interface configuration command.

## Monitoring and Maintaining IP Multicast Routing

These sections describe how to monitor and maintain IP multicast routing:

- Clearing Caches, Tables, and Databases, page 45-61
- Displaying System and Network Statistics, page 45-62
- Monitoring IP Multicast Routing, page 45-63

## Clearing Caches, Tables, and Databases

You can remove all contents of a particular cache, table, or database. Clearing a cache, table, or database might be necessary when the contents of the particular structure are or suspected to be invalid.

You can use any of the privileged EXEC commands in Table 45-5 to clear IP multicast caches, tables, and databases:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>clear ip cgmp</code></td>
<td>Clear all group entries the Catalyst switches have cached.</td>
</tr>
<tr>
<td>`clear ip dvmrp route [ *</td>
<td>route ]`</td>
</tr>
</tbody>
</table>
Displaying System and Network Statistics

You can display specific statistics, such as the contents of IP routing tables, caches, and databases.

**Note**

This release does not support per-route statistics.

You can display information to learn resource utilization and solve network problems. You can also display information about node reachability and discover the routing path your device’s packets are taking through the network.

You can use any of the privileged EXEC commands in Table 45-6 to display various routing statistics:

**Table 45-6 Commands for Displaying System and Network Statistics**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>ping [group-name</td>
<td>group-address]</td>
</tr>
<tr>
<td>show ip dvmrp route [ip-address]</td>
<td>Display the entries in the DVMRP routing table.</td>
</tr>
<tr>
<td>show ip igmp groups [group-name</td>
<td>group-address</td>
</tr>
<tr>
<td>show ip igmp interface [type number]</td>
<td>Display multicast-related information about an interface.</td>
</tr>
<tr>
<td>show ip mcache [group</td>
<td>source]]</td>
</tr>
<tr>
<td>show ip mpacket [source-address</td>
<td>name] [group-address</td>
</tr>
<tr>
<td>show ip mrout [group-name</td>
<td>group-address] [source</td>
</tr>
<tr>
<td>show ip pim interface [type number</td>
<td>count]</td>
</tr>
<tr>
<td>show ip pim neighbor [type number]</td>
<td>List the PIM neighbors discovered by the switch.</td>
</tr>
<tr>
<td>show ip pim rp [group-name</td>
<td>group-address]</td>
</tr>
</tbody>
</table>
Monitoring and Maintaining IP Multicast Routing

You can use the privileged EXEC commands in Table 45-7 to monitor IP multicast routers, packets, and paths:

Table 45-7 Commands for Monitoring IP Multicast Routing

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>mrinfo [hostname</td>
<td>address</td>
</tr>
<tr>
<td>mstat source</td>
<td>destination</td>
</tr>
<tr>
<td>mtrace source</td>
<td>destination</td>
</tr>
</tbody>
</table>

Note:
- The `show ip rpf {source-address | name}` command displays how the switch is doing Reverse-Path Forwarding (that is, from the unicast routing table, DVMRP routing table, or static mroutes).

### Table 45-6 Commands for Displaying System and Network Statistics (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip rpf {source-address</td>
<td>name}</td>
</tr>
</tbody>
</table>
Configuring MSDP

This chapter describes how to configure the Multicast Source Discovery Protocol (MSDP) on the Catalyst 3750 Metro switch. The MSDP connects multiple Protocol-Independent Multicast sparse-mode (PIM-SM) domains.

MSDP is not fully supported in this software release because of a lack of support for Multicast Border Gateway Protocol (MBGP), which works closely with MSDP. However, it is possible to create default peers that MSDP can operate with if MBGP is not running.

Note

For complete syntax and usage information for the commands used in this chapter, see the Cisco IOS IP Command Reference, Volume 3 of 3: Multicast, Release 12.2.

This chapter consists of these sections:

- Understanding MSDP, page 46-1
- Configuring MSDP, page 46-3
- Monitoring and Maintaining MSDP, page 46-17

Understanding MSDP

MSDP allows multicast sources for a group to be known to all rendezvous points (RPs) in different domains. Each PIM-SM domain uses its own RPs and does not depend on RPs in other domains. An RP runs MSDP over the TCP to discover multicast sources in other domains.

An RP in a PIM-SM domain has an MSDP peering relationship with MSDP-enabled devices in another domain. The peering relationship occurs over a TCP connection, primarily exchanging a list of sources sending to multicast groups. The TCP connections between RPs are achieved by the underlying routing system. The receiving RP uses the source lists to establish a source path.

The purpose of this topology is to have domains discover multicast sources in other domains. If the multicast sources are of interest to a domain that has receivers, multicast data is delivered over the normal, source-tree building mechanism in PIM-SM. MSDP is also used to announce sources sending to a group. These announcements must originate at the domain’s RP.

MSDP depends heavily on the Border Gateway Protocol (BGP) or MBGP for interdomain operation. We recommend that you run MSDP in RPs in your domain that are RPs for sources sending to global groups to be announced to the Internet.
MSDP Operation

Figure 46-1 shows MSDP operating between two MSDP peers. PIM uses MSDP as the standard mechanism to register a source with the RP of a domain. When MSDP is configured, this sequence occurs.

When a source sends its first multicast packet, the first-hop router (designated router or RP) directly connected to the source sends a PIM register message to the RP. The RP uses the register message to register the active source and to forward the multicast packet down the shared tree in the local domain. With MSDP configured, the RP also forwards a source-active (SA) message to all MSDP peers. The SA message identifies the source, the group the source is sending to, and the address of the RP or the originator ID (the IP address of the interface used as the RP address), if configured.

Each MSDP peer receives and forwards the SA message away from the originating RP to achieve peer reverse-path flooding (RPF). The MSDP device examines the BGP or MBGP routing table to discover which peer is the next hop toward the originating RP of the SA message. Such a peer is called an RPF peer (reverse-path forwarding peer). The MSDP device forwards the message to all MSDP peers other than the RPF peer. For information on how to configure an MSDP peer when BGP and MBGP are not supported, see the “Configuring a Default MSDP Peer” section on page 46-4.

If the MSDP peer receives the same SA message from a non-RPF peer toward the originating RP, it drops the message. Otherwise, it forwards the message to all its MSDP peers.

The RP for a domain receives the SA message from an MSDP peer. If the RP has any join requests for the group the SA message describes and if the (*.G) entry exists with a nonempty outgoing interface list, the domain is interested in the group, and the RP triggers an (S,G) join toward the source. After the (S,G) join reaches the source’s DR, a branch of the source tree has been built from the source to the RP in the remote domain. Multicast traffic can now flow from the source across the source tree to the RP and then down the shared tree in the remote domain to the receiver.
MSDP Benefits

MSDP has these benefits:

- It breaks up the shared multicast distribution tree. You can make the shared tree local to your domain. Your local members join the local tree, and join messages for the shared tree never need to leave your domain.

- PIM sparse-mode domains can rely only on their own RPs, decreasing reliance on RPs in another domain. This increases security because you can prevent your sources from being known outside your domain.

- Domains with only receivers can receive data without globally advertising group membership.

- Global source multicast routing table state is not required, saving memory.

Configuring MSDP

These sections describe how to configure MSDP:

- Default MSDP Configuration, page 46-4
- Configuring a Default MSDP Peer, page 46-4 (required)
- Caching Source-Active State, page 46-6 (optional)
- Requesting Source Information from an MSDP Peer, page 46-8 (optional)
Default MSDP Configuration

MSDP is not enabled, and no default MSDP peer exists.

Configuring a Default MSDP Peer

In this software release, because BGP and MBGP are not supported, you cannot configure an MSDP peer on the local switch by using the `ip msdp peer` global configuration command. Instead, you define a default MSDP peer (by using the `ip msdp default-peer` global configuration command) from which to accept all SA messages for the switch. The default MSDP peer must be a previously configured MSDP peer. Configure a default MSDP peer when the switch is not BGP- or MBGP-peering with an MSDP peer. If a single MSDP peer is configured, the switch always accepts all SA messages from that peer.

Figure 46-2 shows a network in which default MSDP peers might be used. In Figure 46-2, a customer who owns Switch B is connected to the Internet through two Internet service providers (ISPs), one owning Router A and the other owning Router C. They are not running BGP or MBGP between them. To learn about sources in the ISP’s domain or in other domains, Switch B at the customer site identifies Router A as its default MSDP peer. Switch B advertises SA messages to both Router A and Router C but accepts SA messages only from Router A or only from Router C. If Router A is first in the configuration file, it is used if it is running. If Router A is not running, only then does Switch B accept SA messages from Router C. This is the default behavior without a prefix list.

If you specify a prefix list, the peer is a default peer only for the prefixes in the list. You can have multiple active default peers when you have a prefix list associated with each. When you do not have any prefix lists, you can configure multiple default peers, but only the first one is the active default peer as long as the router has connectivity to this peer and the peer is alive. If the first configured peer fails or the connectivity to this peer fails, the second configured peer becomes the active default, and so on.

The ISP probably uses a prefix list to define which prefixes it accepts from the customer’s router.
Beginning in privileged EXEC mode, follow these steps to specify a default MSDP peer. This procedure is required.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Enter global configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>ip msdp default-peer <em>ip-address</em> *name* *prefix-list <em>list</em></td>
</tr>
<tr>
<td>Define a default peer from which to accept all MSDP SA messages.</td>
<td></td>
</tr>
<tr>
<td>- For <em>ip-address</em> *name*, enter the IP address or Domain Name System (DNS) server name of the MSDP default peer.</td>
<td></td>
</tr>
<tr>
<td>- (Optional) For <em>prefix-list list</em>, enter the list name that specifies the peer to be the default peer only for the listed prefixes. You can have multiple active default peers when you have a prefix list associated with each.</td>
<td></td>
</tr>
</tbody>
</table>

When you enter multiple *ip msdp default-peer* commands with the *prefix-list* keyword, you use all the default peers at the same time for different RP prefixes. This syntax is typically used in a service provider cloud that connects stub site clouds.

When you enter multiple *ip msdp default-peer* commands without the *prefix-list* keyword, a single active peer accepts all SA messages. If that peer fails, the next configured default peer accepts all SA messages. This syntax is typically used at a stub site.
Configuring MSDP

To remove the default peer, use the `no ip msdp default-peer ip-address | name` global configuration command.

This example shows a partial configuration of Router A and Router C in Figure 46-2. Each of these ISPs have more than one customer (like the customer in Figure 46-2) who use default peering (no BGP or MBGP). In that case, they might have similar configurations. That is, they accept SAs only from a default peer if the SA is permitted by the corresponding prefix list.

**Router A**

Router(config)# ip msdp default-peer 10.1.1.1
Router(config)# ip msdp default-peer 10.1.1.1 prefix-list site-a
Router(config)# ip prefix-list site-b permit 10.0.0.0/8

**Router C**

Router(config)# ip msdp default-peer 10.1.1.1 prefix-list site-a
Router(config)# ip prefix-list site-b permit 10.0.0.0/8

### Caching Source-Active State

By default, the switch does not cache source/group pairs from received SA messages. When the switch forwards the MSDP SA information, it does not store it in memory. Therefore, if a member joins a group soon after a SA message is received by the local RP, that member needs to wait until the next SA message to hear about the source. This delay is known as join latency.

If you want to sacrifice some memory in exchange for reducing the latency of the source information, you can configure the switch to cache SA messages.
Beginning in privileged EXEC mode, follow these steps to enable the caching of source/group pairs. This procedure is optional.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>ip msdp cache-sa-state [list access-list-number]</td>
<td>Enable the caching of source/group pairs (create an SA state). Those pairs that pass the access list are cached. For list access-list-number, the range is 100 to 199.</td>
</tr>
</tbody>
</table>
| 3    | access-list access-list-number {deny | permit} protocol source source-wildcard destination destination-wildcard | Create an IP extended access list, repeating the command as many times as necessary.  
  - For access-list-number, the range is 100 to 199. Enter the same number created in Step 2.  
  - The deny keyword denies access if the conditions are matched. The permit keyword permits access if the conditions are matched.  
  - For protocol, enter ip as the protocol name.  
  - For source, enter the number of the network or host from which the packet is being sent.  
  - For source-wildcard, enter the wildcard bits in dotted decimal notation to be applied to the source. Place ones in the bit positions that you want to ignore.  
  - For destination, enter the number of the network or host to which the packet is being sent.  
  - For destination-wildcard, enter the wildcard bits in dotted decimal notation to be applied to the destination. Place ones in the bit positions that you want to ignore.  
  Recall that the access list is always terminated by an implicit deny statement for everything. |
| 4    | end | Return to privileged EXEC mode. |
| 5    | show running-config | Verify your entries. |
| 6    | copy running-config startup-config | (Optional) Save your entries in the configuration file. |

**Note**  
An alternative to this command is the `ip msdp sa-request` global configuration command, which causes the switch to send an SA request message to the MSDP peer when a new member for a group becomes active. For more information, see the next section.

To return to the default setting (no SA state is created), use the `no ip msdp cache-sa-state` global configuration command.

This example shows how to enable the cache state for all sources in 171.69.0.0/16 sending to groups 224.2.0.0/16:

```
Switch(config)# ip msdp cache-sa-state 100
Switch(config)# access-list 100 permit ip 171.69.0.0 0.0.255.255 224.2.0.0 0.0.255.255
```
Requesting Source Information from an MSDP Peer

Local RPs can send SA requests and get immediate responses for all active sources for a given group. By default, the switch does not send any SA request messages to its MSDP peers when a new member joins a group and wants to receive multicast traffic. The new member waits to receive the next periodic SA message.

If you want a new member of a group to learn the active multicast sources in a connected PIM sparse-mode domain that are sending to a group, configure the switch to send SA request messages to the specified MSDP peer when a new member joins a group. The peer replies with the information in its SA cache. If the peer does not have a cache configured, this command has no result. Configuring this feature reduces join latency but sacrifices memory.

Beginning in privileged EXEC mode, follow these steps to configure the switch to send SA request messages to the MSDP peer when a new member joins a group and wants to receive multicast traffic. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip msdp sa-request {ip-address</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
</tr>
<tr>
<td>Step 4</td>
<td>show running-config</td>
</tr>
<tr>
<td>Step 5</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To return to the default setting, use the no ip msdp sa-request {ip-address | name} global configuration command.

This example shows how to configure the switch to send SA request messages to the MSDP peer at 171.69.1.1:

```
Switch(config)# ip msdp sa-request 171.69.1.1
```

Controlling Source Information that Your Switch Originates

You can control the multicast source information that originates with your switch:

- Sources you advertise (based on your sources)
- Receivers of source information (based on knowing the requestor)

For more information, see the “Redistributing Sources” section on page 46-9 and the “Filtering Source-Active Request Messages” section on page 46-10.
**Redistributing Sources**

SA messages originate on RPs to which sources have registered. By default, any source that registers with an RP is advertised. The \textit{A} flag is set in the RP when a source is registered, which means the source is advertised in an SA unless it is filtered.

Beginning in privileged EXEC mode, follow these steps to further restrict which registered sources are advertised. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>ip msdp redistribute [list access-list-name] [asn aspath-access-list-number] [route-map map]</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The switch advertises (S,G) pairs according to the access list or autonomous system path access list.</td>
</tr>
</tbody>
</table>
Filtering Source-Active Request Messages

By default, only switches that are caching SA information can respond to SA requests. By default, such a switch honors all SA request messages from its MSDP peers and supplies the IP addresses of the active sources.

However, you can configure the switch to ignore all SA requests from an MSDP peer. You can also honor only those SA request messages from a peer for groups described by a standard access list. If the groups in the access list pass, SA request messages are accepted. All other such messages from the peer for other groups are ignored.

Beginning in privileged EXEC mode, follow these steps to configure one of these options. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3</td>
<td>Create an IP standard access list, repeating the command as many times as necessary.</td>
</tr>
<tr>
<td>access-list access-list-number {deny</td>
<td>permit} source [source-wildcard] | or access-list access-list-number {deny</td>
</tr>
<tr>
<td>Step 4</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>end</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>show running-config</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

To remove the filter, use the `no ip msdp redistribute` global configuration command.
### Configuring MSDP

To return to the default setting, use the **no ip msdp filter-sa-request** `{ip-address | name}` global configuration command.

This example shows how to configure the switch to filter SA request messages from the MSDP peer at 171.69.2.2. SA request messages from sources on network 192.4.22.0 pass access list 1 and are accepted; all others are ignored.

```
Switch(config)# ip msdp filter sa-request 171.69.2.2 list 1
Switch(config)# access-list 1 permit 192.4.22.0 0.0.0.255
```

### Controlling Source Information that Your Switch Forwards

By default, the switch forwards all SA messages it receives to all its MSDP peers. However, you can prevent outgoing messages from being forwarded to a peer by using a filter or by setting a time-to-live (TTL) value. These methods are described in the next sections.

#### Using a Filter

By creating a filter, you can perform one of these actions:

- Filter all source/group pairs
- Specify an IP extended access list to pass only certain source/group pairs
- Filter based on match criteria in a route map
Beginning in privileged EXEC mode, follow these steps to apply a filter. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip msdp sa-filter out ip-address | name</td>
</tr>
<tr>
<td></td>
<td>or</td>
</tr>
<tr>
<td></td>
<td>ip msdp sa-filter out {ip-address | name} list access-list-number</td>
</tr>
<tr>
<td></td>
<td>or</td>
</tr>
<tr>
<td></td>
<td>ip msdp sa-filter out {ip-address | name} route-map map-tag</td>
</tr>
<tr>
<td>Step 3</td>
<td>access-list access-list-number {deny | permit} protocol source source-wildcard destination destination-wildcard</td>
</tr>
<tr>
<td></td>
<td>• For access-list-number, enter the number specified in Step 2.</td>
</tr>
<tr>
<td></td>
<td>• The deny keyword denies access if the conditions are matched. The permit keyword permits access if the conditions are matched.</td>
</tr>
<tr>
<td></td>
<td>• For protocol, enter ip as the protocol name.</td>
</tr>
<tr>
<td></td>
<td>• For source, enter the number of the network or host from which the packet is being sent.</td>
</tr>
<tr>
<td></td>
<td>• For source-wildcard, enter the wildcard bits in dotted decimal notation to be applied to the source. Place ones in the bit positions that you want to ignore.</td>
</tr>
<tr>
<td></td>
<td>• For destination, enter the number of the network or host to which the packet is being sent.</td>
</tr>
<tr>
<td></td>
<td>• For destination-wildcard, enter the wildcard bits in dotted decimal notation to be applied to the destination. Place ones in the bit positions that you want to ignore.</td>
</tr>
<tr>
<td></td>
<td>Recall that the access list is always terminated by an implicit deny statement for everything.</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
</tr>
<tr>
<td>Step 5</td>
<td>show running-config</td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To remove the filter, use the no ip msdp sa-filter out \{ip-address \| name\} \[list access-list-number\] \[route-map map-tag\] global configuration command.
This example shows how to allow only (S,G) pairs that pass access list 100 to be forwarded in an SA message to the peer named switch.cisco.com:

```
Switch(config)# ip msdp peer switch.cisco.com connect-source gigabitethernet1/0/1
Switch(config)# ip msdp sa-filter out switch.cisco.com list 100
Switch(config)# access-list 100 permit ip 171.69.0.0 0.0.255.255 224.20 0 0.0.255.255
```

### Using TTL to Limit the Multicast Data Sent in SA Messages

You can use a TTL value to control what data is encapsulated in the first SA message for every source. Only multicast packets with an IP-header TTL greater than or equal to the `ttl` argument are sent to the specified MSDP peer. For example, you can limit internal traffic to a TTL of 8. If you want other groups to go to external locations, you must send those packets with a TTL greater than 8.

Beginning in privileged EXEC mode, follow these steps to establish a TTL threshold. This procedure is optional.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
<td></td>
</tr>
</tbody>
</table>
| Step 2 | ip msdp ttl-threshold `ip-address | Limit which multicast data is encapsulated in the first SA message to the specified MSDP peer.  
  | name` `ttl` | 
  | | • For `ip-address | name`, enter the IP address or name of the MSDP peer to which the TTL limitation applies.  
  | | • For `ttl`, enter the TTL value. The default is 0, which means all multicast data packets are forwarded to the peer until the TTL is exhausted. The range is 0 to 255. |
| Step 3 | end | Return to privileged EXEC mode. |
| Step 4 | show running-config | Verify your entries. |
| Step 5 | copy running-config startup-config | (Optional) Save your entries in the configuration file. |

To return to the default setting, use the `no ip msdp ttl-threshold `ip-address | name` global configuration command.

### Controlling Source Information that Your Switch Receives

By default, the switch receives all SA messages that its MSDP RPF peers send to it. However, you can control the source information that you receive from MSDP peers by filtering incoming SA messages. In other words, you can configure the switch to not accept them.

You can perform one of these actions:

- Filter all incoming SA messages from an MSDP peer
- Specify an IP extended access list to pass certain source/group pairs
- Filter based on match criteria in a route map
Beginning in privileged EXEC mode, follow these steps to apply a filter. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 ip msdp sa-filter in ip-address \ name</td>
<td>Filter all SA messages from the specified MSDP peer.</td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td>ip msdp sa-filter in {ip-address \ name}</td>
<td>From the specified peer, pass only those SA messages that pass the IP</td>
</tr>
<tr>
<td>list access-list-number</td>
<td>extended access list. The range for the extended access-list-number is 100 to 199.</td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td>ip msdp sa-filter in {ip-address \ name}</td>
<td>If both the list and the route-map keywords are used, all conditions</td>
</tr>
<tr>
<td>route-map map-tag</td>
<td>must be true to pass any (S,G) pair in incoming SA messages.</td>
</tr>
<tr>
<td>Step 3 access-list access-list-number {deny</td>
<td>(Optional) Create an IP extended access list, repeating the command as</td>
</tr>
<tr>
<td>permit} protocol source source-wildcard</td>
<td>many times as necessary.</td>
</tr>
<tr>
<td>destination destination-wildcard</td>
<td></td>
</tr>
<tr>
<td>For access-list-number, enter the number specified in Step 2.</td>
<td></td>
</tr>
<tr>
<td>The deny keyword denies access if the conditions are matched.</td>
<td></td>
</tr>
<tr>
<td>The permit keyword permits access if the conditions are matched.</td>
<td></td>
</tr>
<tr>
<td>For protocol, enter ip as the protocol name.</td>
<td></td>
</tr>
<tr>
<td>For source, enter the number of the network or host from which the</td>
<td></td>
</tr>
<tr>
<td>packet is being sent.</td>
<td></td>
</tr>
<tr>
<td>For source-wildcard, enter the wildcard bits in dotted decimal</td>
<td></td>
</tr>
<tr>
<td>notation to be applied to the source. Place ones in the bit positions</td>
<td></td>
</tr>
<tr>
<td>that you want to ignore.</td>
<td></td>
</tr>
<tr>
<td>For destination, enter the number of the network or host to which</td>
<td></td>
</tr>
<tr>
<td>the packet is being sent.</td>
<td></td>
</tr>
<tr>
<td>For destination-wildcard, enter the wildcard bits in dotted decimal</td>
<td></td>
</tr>
<tr>
<td>notation to be applied to the destination. Place ones in the bit</td>
<td></td>
</tr>
<tr>
<td>positions that you want to ignore.</td>
<td></td>
</tr>
<tr>
<td>Recall that the access list is always terminated by an implicit deny</td>
<td></td>
</tr>
<tr>
<td>statement for everything.</td>
<td></td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5 show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 6 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To remove the filter, use the no ip msdp sa-filter in \{ip-address \ name\} \[list access-list-number]\[route-map map-tag\] global configuration command.

This example shows how to filter all SA messages from the peer named switch.cisco.com:

```
Switch(config)# ip msdp peer switch.cisco.com connect-source gigabitethernet1/0/1
Switch(config)# ip msdp sa-filter in switch.cisco.com
```
Configuring an MSDP Mesh Group

An MSDP mesh group is a group of MSDP speakers that have fully meshed MSDP connectivity among one another. Any SA messages received from a peer in a mesh group are not forwarded to other peers in the same mesh group. Thus, you reduce SA message flooding and simplify peer-RPF flooding. Use the `ip msdp mesh-group` global configuration command when there are multiple RPs within a domain. It is especially used to send SA messages across a domain. You can configure multiple mesh groups (with different names) in a single switch.

Beginning in privileged EXEC mode, follow these steps to create a mesh group. This procedure is optional.

**Command** | **Purpose**
--- | ---
**Step 1** | configure terminal
Enter global configuration mode.
**Step 2** | `ip msdp mesh-group name {ip-address | name}`
Configure an MSDP mesh group, and specify the MSDP peer belonging to that mesh group.
By default, the MSDP peers do not belong to a mesh group.
- For `name`, enter the name of the mesh group.
- For `ip-address | name`, enter the IP address or name of the MSDP peer to be a member of the mesh group.
**Step 3** | `end`
Return to privileged EXEC mode.
**Step 4** | `show running-config`
Verify your entries.
**Step 5** | `copy running-config startup-config` (Optional) Save your entries in the configuration file.
**Step 6** | Repeat this procedure on each MSDP peer in the group.

To remove an MSDP peer from a mesh group, use the `no ip msdp mesh-group name {ip-address | name}` global configuration command.

Shutting Down an MSDP Peer

If you want to configure many MSDP commands for the same peer and you do not want the peer to become active, you can shut down the peer, configure it, and later bring it up. When a peer is shut down, the TCP connection is terminated and is not restarted. You can also shut down an MSDP session without losing configuration information for the peer.

Beginning in privileged EXEC mode, follow these steps to shut down a peer. This procedure is optional.

**Command** | **Purpose**
--- | ---
**Step 1** | configure terminal
Enter global configuration mode.
**Step 2** | `ip msdp shutdown {peer-name | peer address}`
Administratively shut down the specified MSDP peer without losing configuration information.
For `peer-name | peer address`, enter the IP address or name of the MSDP peer to shut down.
**Step 3** | `end`
Return to privileged EXEC mode.
To bring the peer back up, use the `no ip msdp shutdown {peer-name | peer address}` global configuration command. The TCP connection is reestablished.

### Including a Bordering PIM Dense-Mode Region in MSDP

You can configure MSDP on a switch that borders a PIM sparse-mode region with a dense-mode region. By default, active sources in the dense-mode region do not participate in MSDP.

**Note**

We do not recommend using the `ip msdp border sa-address` global configuration command. It is better to configure the border router in the sparse-mode domain to proxy-register sources in the dense-mode domain to the RP of the sparse-mode domain and have the sparse-mode domain use standard MSDP procedures to advertise these sources.

Beginning in privileged EXEC mode, follow these steps to configure the border router to send SA messages for sources active in the dense-mode region to the MSDP peers. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>ip msdp border sa-address interface-id</code></td>
<td>Configure the switch on the border between a dense-mode and sparse-mode region to send SA messages about active sources in the dense-mode region. For <code>interface-id</code>, specify the interface from which the IP address is derived and used as the RP address in SA messages. The IP address of the interface is used as the Originator-ID, which is the RP field in the SA message.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>ip msdp redistribute [list access-list-name] [asn aspath-access-list-number] [route-map map]</code></td>
<td>Configure which (S,G) entries from the multicast routing table are advertised in SA messages. For more information, see the “Redistributing Sources” section on page 46-9.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td><code>show running-config</code></td>
<td>Verify your entries.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Note that the `ip msdp originator-id` global configuration command also identifies an interface to be used as the RP address. If you configure both the `ip msdp border sa-address` and the `ip msdp originator-id` global configuration commands, the address derived from the `ip msdp originator-id` command determines the RP address.

To return to the default setting (active sources in the dense-mode region do not participate in MSDP), use the `no ip msdp border sa-address interface-id` global configuration command.
Configuring an Originating Address other than the RP Address

You can allow an MSDP speaker that originates an SA message to use the IP address of the interface as the RP address in the SA message by changing the Originator ID. You might change the Originator ID in one of these cases:

- If you configure a logical RP on multiple switches in an MSDP mesh group.
- If you have a switch that borders a PIM sparse-mode domain and a dense-mode domain. If a switch borders a dense-mode domain for a site, and sparse-mode is being used externally, you might want dense-mode sources to be known to the outside world. Because this switch is not an RP, it would not have an RP address to use in an SA message. Therefore, this command provides the RP address by specifying the address of the interface.

Beginning in privileged EXEC mode, follow these steps to allow an MSDP speaker that originates an SA message to use the IP address on the interface as the RP address in the SA message. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 ip msdp originator-id interface-id</td>
<td>Configures the RP address in SA messages to be the address of the originating device interface. For interface-id, specify the interface on the local switch.</td>
</tr>
<tr>
<td>Step 3 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4 show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 5 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

If you configure both the `ip msdp border sa-address` and the `ip msdp originator-id` global configuration commands, the address derived from the `ip msdp originator-id` command determines the address of the RP.

To prevent the RP address from being derived in this way, use the `no ip msdp originator-id interface-id` global configuration command.

Monitoring and Maintaining MSDP

To monitor MSDP SA messages, peers, state, or peer status, use one or more of the privileged EXEC commands in Table 46-1:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ip msdp [peer-address</td>
<td>name] [detail] [routes]</td>
</tr>
<tr>
<td>debug ip msdp resets</td>
<td>debugs MSDP peer reset reasons.</td>
</tr>
<tr>
<td>show ip msdp count [autonomous-system-number]</td>
<td>displays the number of sources and groups originated in SA messages from each autonomous system. The <code>ip msdp cache-sa-state</code> command must be configured for this command to produce any output.</td>
</tr>
</tbody>
</table>
To clear MSDP connections, statistics, or SA cache entries, use the privileged EXEC commands in Table 46-2:

### Table 46-2 Commands for Clearing MSDP Connections, Statistics, or SA Cache Entries

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip msdp peer peer-address</td>
<td>Clears the TCP connection to the specified MSDP peer, resetting all MSDP message counters.</td>
</tr>
<tr>
<td>clear ip msdp statistics [peer-address]</td>
<td>Clears statistics counters for one or all the MSDP peers without resetting the sessions.</td>
</tr>
<tr>
<td>clear ip msdp sa-cache [group-address]</td>
<td>Clears the SA cache entries for all entries, all sources for a specific group, or all entries for a specific source/group pair.</td>
</tr>
</tbody>
</table>

### Table 46-1 Commands for Monitoring and Maintaining MSDP (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip msdp peer [peer-address</td>
<td>Displays detailed information about an MSDP peer.</td>
</tr>
<tr>
<td>show ip msdp sa-cache [group-address</td>
<td>Displays (S,G) state learned from MSDP peers.</td>
</tr>
<tr>
<td>show ip msdp summary</td>
<td>Displays MSDP peer status and SA message counts.</td>
</tr>
</tbody>
</table>

To clear MSDP connections, statistics, or SA cache entries, use the privileged EXEC commands in Table 46-2:
Configuring Fallback Bridging

This chapter describes how to configure fallback bridging (VLAN bridging) on the Catalyst 3750 Metro switch. With fallback bridging, you can forward non-IP packets that the switch does not route between VLAN bridge domains and routed ports.

For complete syntax and usage information for the commands used in this chapter, see the Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2, Release 12.2.

This chapter consists of these sections:

- Understanding Fallback Bridging, page 47-1
- Configuring Fallback Bridging, page 47-2
- Monitoring and Maintaining Fallback Bridging, page 47-10

Understanding Fallback Bridging

With fallback bridging, the switch bridges together two or more VLANs or routed ports, essentially connecting multiple VLANs within one bridge domain. Fallback bridging forwards traffic that the switch does not route and forwards traffic belonging to a nonroutable protocol such as DECnet.

A VLAN bridge domain is represented with switch virtual interfaces (SVIs). A set of SVIs and routed ports (which do not have any VLANs associated with them) can be configured (grouped together) to form a bridge group. Recall that an SVI represents a VLAN of switch ports as one interface to the routing or bridging function in the system. You associate only one SVI with a VLAN, and you configure an SVI for a VLAN only when you want to route between VLANs, to fallback-bridge nonroutable protocols between VLANs, or to provide IP host connectivity to the switch. A routed port is a physical port that acts like a port on a router, but it is not connected to a router. A routed port is not associated with a particular VLAN, does not support VLAN subinterfaces, but behaves like a normal routed port. For more information about SVIs and routed ports, see Chapter 9, “Configuring Interface Characteristics.”

A bridge group is an internal organization of network interfaces on a switch. You cannot use bridge groups to identify traffic switched within the bridge group outside the switch on which they are defined. Bridge groups on the switch function as distinct bridges; that is, bridged traffic and bridge protocol data units (BPDUs) are not exchanged between different bridge groups on a switch.

Fallback bridging does not allow the spanning trees from the VLANs being bridged to collapse. Each VLAN has its own spanning-tree instance and a separate spanning tree, called the VLAN-bridge spanning tree, which runs on top of the bridge group to prevent loops.
The switch creates a VLAN-bridge spanning-tree instance when a bridge group is created. The switch runs the bridge group and treats the SVIs and routed ports in the bridge group as its spanning-tree ports. These are the reasons for placing network interfaces into a bridge group:

- To bridge all nonrouted traffic among the network interfaces making up the bridge group. If the packet destination address is in the bridge table, the packet is forwarded on a single interface in the bridge group. If the packet destination address is not in the bridge table, the packet is flooded on all forwarding interfaces in the bridge group. A source MAC address is learned on a bridge group only when the address is learned on a VLAN (the reverse is not true).

- To participate in the spanning-tree algorithm by receiving, and in some cases sending, BPDUs on the LANs to which they are attached. A separate spanning-tree process runs for each configured bridge group. Each bridge group participates in a separate spanning-tree instance. A bridge group establishes a spanning-tree instance based on the BPDUs it receives on only its member ports. If the bridge STP BPDU is received on a port whose VLAN does not belong to a bridge group, the BPDU is flooded on all the forwarding ports of the VLAN.

Figure 47-1 shows a fallback bridging network example. The switch has two ports configured as SVIs with different assigned IP addresses and attached to two different VLANs. Another port is configured as a routed port with its own IP address. If all three of these ports are assigned to the same bridge group, non-IP protocol frames can be forwarded among the end stations connected to the switch even though they are on different networks and in different VLANs. IP addresses do not need to be assigned to routed ports or SVIs for fallback bridging to work.

**Figure 47-1  Fallback Bridging Network Example**

These sections describe how to configure fallback bridging on your switch:

- Default Fallback Bridging Configuration, page 47-3
- Fallback Bridging Configuration Guidelines, page 47-3
- Creating a Bridge Group, page 47-3 (required)
- Adjusting Spanning-Tree Parameters, page 47-5 (optional)
Default Fallback Bridging Configuration

Table 47-1 shows the default fallback bridging configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bridge groups</td>
<td>None are defined or assigned to a port. No VLAN-bridge STP is defined.</td>
</tr>
<tr>
<td>Switch forwards frames for stations that it has dynamically learned</td>
<td>Enabled.</td>
</tr>
<tr>
<td>Spanning tree parameters:</td>
<td></td>
</tr>
<tr>
<td>• Switch priority</td>
<td>• 32768.</td>
</tr>
<tr>
<td>• Port priority</td>
<td>• 128.</td>
</tr>
<tr>
<td>• Port path cost</td>
<td>• 10 Mbps: 100.</td>
</tr>
<tr>
<td></td>
<td>100 Mbps: 19.</td>
</tr>
<tr>
<td></td>
<td>1000 Mbps: 4.</td>
</tr>
<tr>
<td>• Hello BPDU interval</td>
<td>• 2 seconds.</td>
</tr>
<tr>
<td>• Forward-delay interval</td>
<td>• 20 seconds.</td>
</tr>
<tr>
<td>• Maximum idle interval</td>
<td>• 30 seconds.</td>
</tr>
</tbody>
</table>

Fallback Bridging Configuration Guidelines

Up to 32 bridge groups can be configured on the switch.

An interface (an SVI or routed port) can be a member of only one bridge group.

Use a bridge group for each separately bridged (topologically distinct) network connected to the switch.

Do not configure fallback bridging on a switch configured with private VLANs.

All protocols except IP (Version 4 and Version 6), Address Resolution Protocol (ARP), reverse ARP (RARP), LOOPBACK, Frame Relay ARP, and shared STP packets are fallback bridged.

Creating a Bridge Group

To configure fallback bridging for a set of SVIs or routed ports, these interfaces must be assigned to bridge groups. All interfaces in the same group belong to the same bridge domain. Each SVI or routed port can be assigned to only one bridge group.

Note

The protected port feature is not compatible with fallback bridging. When fallback bridging is enabled, it is possible for packets to be forwarded from one protected port on a switch to another protected port on the same switch if the ports are in different VLANs.
Beginning in privileged EXEC mode, follow these steps to create a bridge group and to assign an interface to it. This procedure is required.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>bridge bridge-group protocol vlan-bridge</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>bridge-group bridge-group</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>show running-config</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To remove a bridge group, use the no bridge bridge-group global configuration command. The no bridge bridge-group command automatically removes all SVIs and routed ports from that bridge group. To remove an interface from a bridge group and to remove the bridge group, use the no bridge-group bridge-group interface configuration command.

This example shows how to create bridge group 10, to specify that the VLAN-bridge STP runs in the bridge group, to define a port as a routed port, and to assign the port to the bridge group:

```
Switch(config)# bridge 10 protocol vlan-bridge
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# no shutdown
Switch(config-if)# bridge-group 10
```

This example shows how to create bridge group 10 and to specify that the VLAN-bridge STP runs in the bridge group. It defines a port as an SVI and assigns this port to VLAN 2 and to the bridge group:

```
Switch(config)# bridge 10 protocol vlan-bridge
Switch(config)# vlan 2
Switch(config-vlan)# exit
Switch(config)# interface vlan 2
Switch(config-if)# bridge-group 10
```
Adjusting Spanning-Tree Parameters

You might need to adjust certain spanning-tree parameters if the default values are not suitable. You configure parameters affecting the entire spanning tree by using variations of the `bridge` global configuration command. You configure port-specific parameters by using variations of the `bridge-group` interface configuration command.

You can adjust spanning-tree parameters by performing any of the tasks in these sections:

- Changing the VLAN-Bridge Spanning-Tree Priority, page 47-5 (optional)
- Changing the Interface Priority, page 47-6 (optional)
- Assigning a Path Cost, page 47-7 (optional)
- Adjusting BPDU Intervals, page 47-7 (optional)
- Disabling the Spanning Tree on an Interface, page 47-9 (optional)

**Note**

Only network administrators with a good understanding of how switches and STP function should make adjustments to spanning-tree parameters. Poorly planned adjustments can have a negative impact on performance. A good source on switching is the IEEE 802.1D specification. For more information, see the “References and Recommended Reading” appendix in the *Cisco IOS Configuration Fundamentals Command Reference*.

Changing the VLAN-Bridge Spanning-Tree Priority

You can globally configure the VLAN-bridge spanning-tree priority of a switch when it ties with another switch for the position as the root switch. You also can configure the likelihood that the switch will be selected as the root switch.

Beginning in privileged EXEC mode, follow these steps to change the switch priority. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>bridge bridge-group priority number</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>end</td>
</tr>
</tbody>
</table>
Chapter 47      Configuring Fallback Bridging

Configuring Fallback Bridging

To return to the default setting, use the `no bridge bridge-group priority` global configuration command.

To change the priority on a port, use the `bridge-group priority` interface configuration command (described in the next section).

This example shows how to set the switch priority to 100 for bridge group 10:

```
Switch(config)# bridge 10 priority 100
```

Changing the Interface Priority

You can change the priority for a port. When two switches tie for position as the root switch, you configure a port priority to break the tie. The switch with the lowest port value is elected.

Beginning in privileged EXEC mode, follow these steps to change the port priority. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Specify the port to set the priority, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3 bridge-group bridge-group priority number</td>
<td>Change the priority of a port.</td>
</tr>
<tr>
<td></td>
<td>• For <code>bridge-group</code>, specify the bridge group number. The range is 1 to 255.</td>
</tr>
<tr>
<td></td>
<td>• For <code>number</code>, enter a number from 0 to 255 in increments of 4. The lower the number, the more likely that the port on the switch will be chosen as the root. The default is 128.</td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5 show running-config</td>
<td>Verify your entry.</td>
</tr>
<tr>
<td>Step 6 copy running-config startup-config</td>
<td>(Optional) Save your entry in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default setting, use the `no bridge-group bridge-group priority` interface configuration command.

This example shows how to change the priority to 20 on a port in bridge group 10:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# bridge-group 10 priority 20
```
Configuring Fallback Bridging

Assigning a Path Cost

Each port has a path cost associated with it. By convention, the path cost is 1000/data rate of the attached LAN, in Mbps.

Beginning in privileged EXEC mode, follow these steps to assign a path cost. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>interface interface-id</td>
<td>Specify the port to set the path cost, and enter interface configuration mode.</td>
</tr>
<tr>
<td>bridge-group bridge-group path-cost cost</td>
<td>Assign the path cost of a port.</td>
</tr>
<tr>
<td></td>
<td>• For bridge-group, specify the bridge group number. The range is 1 to 255.</td>
</tr>
<tr>
<td></td>
<td>• For cost, enter a number from 0 to 65535. The higher the value, the higher the cost.</td>
</tr>
<tr>
<td></td>
<td>– For 10 Mbps, the default path cost is 100.</td>
</tr>
<tr>
<td></td>
<td>– For 100 Mbps, the default path cost is 19.</td>
</tr>
<tr>
<td></td>
<td>– For 1000 Mbps, the default path cost is 4.</td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>show running-config</td>
<td>Verify your entry.</td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entry in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default path cost, use the no bridge-group bridge-group path-cost interface configuration command.

This example shows how to change the path cost to 20 on a port in bridge group 10:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# bridge-group 10 path-cost 20
```

Adjusting BPDU Intervals

You can adjust BPDU intervals as described in these sections:

- Adjusting the Interval between Hello BPDU, page 47-8 (optional)
- Changing the Forward-Delay Interval, page 47-8 (optional)
- Changing the Maximum-Idle Interval, page 47-9 (optional)

**Note**

Each switch in a spanning tree adopts the interval between hello BPDU, the forward delay interval, and the maximum idle interval parameters of the root switch, regardless of what its individual configuration might be.
### Adjusting the Interval between Hello BPDUs

Beginning in privileged EXEC mode, follow these step to adjust the interval between hello BPDUs. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> bridge bridge-group hello-time seconds</td>
<td>Specify the interval between hello BPDUs.</td>
</tr>
<tr>
<td></td>
<td>• For bridge-group, specify the bridge group number. The range is 1 to 255.</td>
</tr>
<tr>
<td></td>
<td>• For seconds, enter a number from 1 to 10. The default is 2.</td>
</tr>
<tr>
<td><strong>Step 3</strong> end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong> show running-config</td>
<td>Verify your entry.</td>
</tr>
<tr>
<td><strong>Step 5</strong> copy running-config startup-config</td>
<td>(Optional) Save your entry in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default setting, use the `no bridge bridge-group hello-time` global configuration command.

This example shows how to change the hello interval to 5 seconds in bridge group 10:

```
Switch(config)# bridge 10 hello-time 5
```

### Changing the Forward-Delay Interval

The forward-delay interval is the amount of time spent listening for topology change information after a port has been activated for switching and before forwarding actually begins.

Beginning in privileged EXEC mode, follow these steps to change the forward-delay interval. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> bridge bridge-group forward-time seconds</td>
<td>Specify the forward-delay interval.</td>
</tr>
<tr>
<td></td>
<td>• For bridge-group, specify the bridge group number. The range is 1 to 255.</td>
</tr>
<tr>
<td></td>
<td>• For seconds, enter a number from 4 to 200. The default is 20.</td>
</tr>
<tr>
<td><strong>Step 3</strong> end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong> show running-config</td>
<td>Verify your entry.</td>
</tr>
<tr>
<td><strong>Step 5</strong> copy running-config startup-config</td>
<td>(Optional) Save your entry in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default setting, use the `no bridge bridge-group forward-time` global configuration command.

This example shows how to change the forward-delay interval to 10 seconds in bridge group 10:

```
Switch(config)# bridge 10 forward-time 10
```
Changing the Maximum-Idle Interval

If a switch does not receive BPDUs from the root switch within a specified interval, it recomputes the spanning-tree topology.

Beginning in privileged EXEC mode, follow these steps to change the maximum-idle interval (maximum aging time). This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>bridge bridge-group max-age seconds</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>show running-config</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To return to the default setting, use the no bridge bridge-group max-age global configuration command.

This example shows how to change the maximum-idle interval to 30 seconds in bridge group 10:

\[
\text{Switch(config)}\# \text{bridge 10 max-age 30}
\]

Disabling the Spanning Tree on an Interface

When a loop-free path exists between any two switched subnetworks, you can prevent BPDUs generated in one switching subnetwork from impacting devices in the other switching subnetwork, yet still permit switching throughout the network as a whole. For example, when switched LAN subnetworks are separated by a WAN, BPDUs can be prevented from traveling across the WAN link.

Beginning in privileged EXEC mode, follow these steps to disable spanning tree on a port. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>bridge-group bridge-group spanning-disabled</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>show running-config</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To re-enable spanning tree on the port, use the no bridge-group bridge-group spanning-disabled interface configuration command.
This example shows how to disable spanning tree on a port in bridge group 10:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# bridge group 10 spanning-disabled
```

### Monitoring and Maintaining Fallback Bridging

To monitor and maintain the network, use one or more of the privileged EXEC commands in Table 47-2:

#### Table 47-2 Commands for Monitoring and Maintaining Fallback Bridging

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear bridge bridge-group</td>
<td>Removes any learned entries from the forwarding database.</td>
</tr>
<tr>
<td>show bridge [bridge-group] group</td>
<td>Displays details about the bridge group.</td>
</tr>
<tr>
<td>show bridge [bridge-group] [interface-id</td>
<td>mac-address</td>
</tr>
</tbody>
</table>

For information about the fields in these displays, see the *Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2, Release 12.2*. 
Troubleshooting

This chapter describes how to identify and resolve software problems related to the Cisco IOS software on the Catalyst 3750 Metro switch. Additional troubleshooting information is provided in the hardware installation guide.

For complete syntax and usage information for the commands used in this chapter, see the command reference for this release and the Cisco IOS Command Summary, Release 12.2.

This chapter consists of these sections:

- Recovering from Corrupted Software By Using the XMODEM Protocol, page 48-2
- Recovering from a Lost or Forgotten Password, page 48-3

Note Recovery procedures require that you have physical access to the switch.

- Preventing Autonegotiation Mismatches, page 48-7
- SFP Module Security and Identification, page 48-7
- Monitoring SFP Module Status, page 48-8
- Using Ping, page 48-8
- Using Layer 2 Traceroute, page 48-9
- Using IP Traceroute, page 48-11
- Using Debug Commands, page 48-13
- Using the show platform forward Command, page 48-14
- Using the crashinfo File, page 48-17
Recovering from Corrupted Software By Using the XMODEM Protocol

Switch software can be corrupted during an upgrade, by downloading the wrong file to the switch, and by deleting the image file. In all of these cases, the switch does not pass the power-on self-test (POST), and there is no connectivity.

This 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.

This recovery procedure requires that you have physical access to the switch.

---

**Step 1**
From your PC, download the software image tar file (*image_filename.tar*) from Cisco.com.

The Cisco IOS image is stored as a bin file in a directory in the tar file. For information about locating the software image files on Cisco.com, see the release notes.

**Step 2**
Extract the bin file from the tar file.

- If you are using Windows, use a zip program that is capable of reading a tar file. Use the zip program to navigate to and extract the bin file.
- If you are using UNIX, follow these steps:
  1. Display the contents of the tar file by using the `tar -tvf <image_filename.tar>` UNIX command.
  2. Locate the bin file name in the display and extract it by using the `tar -xvf <image_filename.tar> <image_filename.bin>` UNIX command.

```
switch% tar -xvf image_filename.tar image_filename.bin
```

  3. Verify that the bin file was extracted by using the `ls -l <image_filename.bin>` UNIX command. The bin file name (*image_filename.bin*) should appear in the output.

```
switch% ls -l image_filename.bin
```

**Step 3**
Connect your PC with terminal-emulation software supporting the XMODEM Protocol to the switch console port.

**Step 4**
Set the line speed on the emulation software to 9600 baud.

**Step 5**
Unplug the switch power cord.

**Step 6**
Press 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 1 goes off. Several lines of information about the software appear along with 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
load_helper
boot
```

**Step 7**
Initialize the Flash file system:

```
switch: flash_init
```

**Step 8**
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.
Recovering from a Lost or Forgotten Password

The default configuration for the switch allows an end user with physical access to the switch to recover from a lost password by interrupting the boot process during power-on and by entering a new password. These recovery procedures require that you have physical access to the switch.

Note

On these switches, a system administrator can disable some of the functionality of this feature by allowing an end user to reset a password only by agreeing to return to the default configuration. If you are an end user trying to reset a password when password recovery has been disabled, a status message shows this during the recovery process.

This section describes how to recover a forgotten or lost switch password. It provides two solutions:

- Procedure with Password Recovery Enabled, page 48-4
- Procedure with Password Recovery Disabled, page 48-5

You enable or disable password recovery by using the service password-recovery global configuration command.

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 switch console port.

**Step 2**
Set the line speed on the emulation software to 9600 baud.

**Step 3**
Power off the switch.

**Step 4**
Press 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 1 turns off. Several lines of information about the software appear with instructions, informing you if the password recovery procedure has been disabled or not.

- If you see a message that begins with this:
The system has been interrupted prior to initializing the flash file system. The following commands will initialize the flash file system:

proceed to the “Procedure with Password Recovery Enabled” section on page 48-4, and follow the steps.

- If you see a message that begins with this:

  The password-recovery mechanism has been triggered, but is currently disabled.

  proceed to the “Procedure with Password Recovery Disabled” section on page 48-5, and follow the steps.

**Step 5**  After recovering the password, reload the switch:

```sh
Switch> reload
Proceed with reload? [confirm] y
```

---

**Procedure with Password Recovery Enabled**

If the password-recovery mechanism is enabled, this message appears:

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`
- `load_helper`
- `boot`

**Step 1**  Initialize the Flash file system:

```sh
switch: flash_init
```

**Step 2**  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 3**  Load any helper files:

```sh
switch: load_helper
```

**Step 4**  Display the contents of Flash memory:

```sh
switch: dir flash:
```

The switch file system appears in the directory.

**Step 5**  Rename the configuration file to config.text.old. This file contains the password definition.

```sh
switch: rename flash:config.text flash:config.text.old
```

**Step 6**  Boot the system:

```sh
switch: boot
```

You are prompted to start the setup program. Enter N at the prompt:

```
Continue with the configuration dialog? [yes/no]: N
```

**Step 7**  At the switch prompt, enter privileged EXEC mode:
Switch> enable

Step 8 Rename the configuration file to its original name:
Switch# rename flash:config.text.old flash:config.text

Step 9 Copy the configuration file into memory:
Switch# copy flash:config.text system:running-config
Press Return in response to the confirmation prompts.
The configuration file is now reloaded, and you can change the password.

Step 10 Enter global configuration mode:
Switch# configure terminal

Step 11 Change the password:
Switch (config)# enable secret password
The secret password can be from 1 to 25 alphanumeric characters, can start with a number, is case sensitive, and allows spaces but ignores leading spaces.

Step 12 Return to privileged EXEC mode:
Switch (config)# exit
Switch#

Step 13 Write the running configuration to the startup configuration file:
Switch# copy running-config startup-config
The new password is now in the startup configuration.

Note This procedure is likely to leave your switch virtual interface in a shutdown state. You can see which interface is in this state by entering the show running-config privileged EXEC command. To re-enable the interface, enter the interface vlan vlan-id global configuration command, and specify the VLAN ID of the shutdown interface. With the switch in interface configuration mode, enter the no shutdown command.

Step 14 Reload the switch:
Switch# reload

Procedure with Password Recovery Disabled

If the password-recovery mechanism is disabled, this message appears:
The password-recovery mechanism has been triggered, but is currently disabled. Access to the boot loader prompt through the password-recovery mechanism is disallowed at this point. However, if you agree to let the system be reset back to the default system configuration, access to the boot loader prompt can still be allowed.
Would you like to reset the system back to the default configuration (y/n)?

**Caution**

Returning the switch to the default configuration results in the loss of all existing configurations. We recommend that you contact your system administrator to verify if there are backup switch and VLAN configuration files.

- If you enter **n** (no), the normal boot process continues as if the **Mode** button had not been pressed; you cannot access the boot loader prompt, and you cannot enter a new password. You see the message:
  
  Press Enter to continue........

- If you enter **y** (yes), the configuration file in Flash memory and the VLAN database file are deleted. When the default configuration loads, you can reset the password.

**Step 1**

Elect to continue with password recovery and lose the existing configuration:

Would you like to reset the system back to the default configuration (y/n)? **y**

**Step 2**

Load any helper files:

*Switch*: `load_helper`

**Step 3**

Display the contents of Flash memory:

*switch*: `dir flash`:

The switch file system appears in the directory.

**Step 4**

Boot the system:

*Switch*: `boot`

You are prompted to start the setup program. To continue with password recovery, enter **N** at the prompt:

Continue with the configuration dialog? [yes/no]: **N**

**Step 5**

At the switch prompt, enter privileged EXEC mode:

*Switch*: `enable`

**Step 6**

Enter global configuration mode:

*Switch*: `configure terminal`

**Step 7**

Change the password:

*Switch* (config)# `enable secret password`

The secret password can be from 1 to 25 alphanumeric characters, can start with a number, is case sensitive, and allows spaces but ignores leading spaces.

**Step 8**

Return to privileged EXEC mode:

*Switch* (config)# `exit`

*Switch*#

**Step 9**

Write the running configuration to the startup configuration file:

*Switch*: `copy running-config startup-config`

The new password is now in the startup configuration.
Preventing Autonegotiation Mismatches

The IEEE 802.3ab autonegotiation protocol manages the switch settings for speed (10 Mbps, 100 Mbps, and 1000 Mbps, excluding SFP module ports unless the 1000-BASE-T SFP is installed) 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 set to 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 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.

SFP Module Security and Identification

Cisco small form-factor pluggable (SFP) modules have a serial EEPROM that contains the module serial number, the vendor name and ID, a unique security code, and cyclic redundancy check (CRC). When an SFP module is inserted in the switch, the switch software reads the EEPROM to verify the serial number, vendor name and vendor ID, and recompute the security code and CRC. If the serial number, the vendor name or vendor ID, the security code, or CRC is invalid, the software generates a security error message and places the interface in an error-disabled state.

Note

The security error message references the GBIC_SECURITY facility. The switch supports SFP modules and does not support GBIC modules. Although the error message text refers to GBIC interfaces and modules, the security messages actually refer to the SFP modules and module interfaces. For more information about error messages, see the system message guide for this release.
If you are using a non-Cisco SFP module, remove the SFP module from the switch, and replace it with a Cisco module. After inserting a Cisco SFP module, use the `errdisable recovery cause gbic-invalid` global configuration command to verify the port status, and enter a time interval for recovering from the error-disabled state. After the elapsed interval, the switch brings the interface out of the error-disabled state and retries the operation. For more information about the `errdisable recovery` command, see the command reference for this release.

If the module is identified as a Cisco SFP module, but the system is unable to read vendor-data information to verify its accuracy, an SFP module error message is generated. In this case, you should remove and re-insert the SFP module. If it continues to fail, the SFP module might be defective.

---

**Monitoring SFP Module Status**

You can check the physical or operational status of an SFP module by using the `show interfaces transceiver` privileged EXEC command. This command shows the operational status, such as the temperature and the current for an SFP module on a specific interface and the alarm status. You can also use the command to check the speed and the duplex settings on an SFP module. For more information, see the `show interfaces transceiver` command in the command reference for this release.

---

**Using Ping**

This section consists of this information:

- Understanding Ping, page 48-8
- Executing Ping, page 48-8

---

**Understanding Ping**

The switch supports IP ping, which you can use to test connectivity to remote hosts. Ping sends an echo request packet to an address and waits for a reply. Ping returns one of these responses:

- Normal response—The normal response (`hostname` is alive) occurs in 1 to 10 seconds, depending on network traffic.
- Destination does not respond—If the host does not respond, a `no-answer` message is returned.
- Unknown host—If the host does not exist, an `unknown host` message is returned.
- Destination unreachable—If the default gateway cannot reach the specified network, a `destination-unreachable` message is returned.
- Network or host unreachable—If there is no entry in the route table for the host or network, a `network or host unreachable` message is returned.

---

**Executing Ping**

If you attempt to ping a host in a different IP subnetwork, you must define a static route to the network or have IP routing configured to route between those subnets. For more information, see Chapter 36, “Configuring IP Unicast Routing.”
IP routing is disabled by default on all switches. If you need to enable or configure IP routing, see Chapter 36, “Configuring IP Unicast Routing.”

Beginning in privileged EXEC mode, use this command to ping another device on the network from the switch:

Beginning in privileged EXEC mode, use this command to ping another device on the network from the switch:

```
ping ip host \ address
```

Table 48-1 describes the possible ping character output.

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>!</td>
<td>Each exclamation point means receipt of a reply.</td>
</tr>
<tr>
<td>.</td>
<td>Each period means the network server timed out while waiting for a reply.</td>
</tr>
<tr>
<td>U</td>
<td>A destination unreachable error PDU was received.</td>
</tr>
<tr>
<td>C</td>
<td>A congestion experienced packet was received.</td>
</tr>
<tr>
<td>I</td>
<td>User interrupted test.</td>
</tr>
<tr>
<td>?</td>
<td>Unknown packet type.</td>
</tr>
<tr>
<td>&amp;</td>
<td>Packet lifetime exceeded.</td>
</tr>
</tbody>
</table>

To terminate a ping session, enter the escape sequence (Ctrl-^ X by default). You enter the default by simultaneously pressing and releasing the Ctrl, Shift, and 6 keys, and then pressing the X key.

Using Layer 2 Traceroute

This section describes this information:

- Understanding Layer 2 Traceroute, page 48-10
- Usage Guidelines, page 48-10
- Displaying the Physical Path, page 48-11
Understanding Layer 2 Traceroute

The Layer 2 traceroute feature allows the switch to identify the physical path that a packet takes from a source device to a destination device. Layer 2 traceroute supports only unicast source and destination MAC addresses. It determines the path by using the MAC address tables of the switches in the path. When the switch detects a device in the path that does not support Layer 2 traceroute, the switch continues to send Layer 2 trace queries and lets them time out.

The switch can only identify the path from the source device to the destination device. It cannot identify the path that a packet takes from source host to the source device or from the destination device to the destination host.

Usage Guidelines

These are the Layer 2 traceroute usage guidelines:

- Cisco Discovery Protocol (CDP) must be enabled on all the devices in the network. For Layer 2 traceroute to function properly, do not disable CDP. If any devices in the physical path are transparent to CDP, the switch cannot identify the path through these devices.

  *Note* For more information about enabling CDP, see Chapter 25, “Configuring CDP.”

- A switch is reachable from another switch when you can test connectivity by using the `ping` privileged EXEC command. All switches in the physical path must be reachable from each other.
- The maximum number of hops identified in the path is ten.
- You can enter the `traceroute mac` or the `traceroute mac ip` privileged EXEC command on a switch that is not in the physical path from the source device to the destination device. All switches in the path must be reachable from this switch.
- The `traceroute mac` command output shows the Layer 2 path only when the specified source and destination MAC addresses belong to the same VLAN. If you specify source and destination MAC addresses that belong to different VLANs, the Layer 2 path is not identified, and an error message appears.
- If you specify a multicast source or destination MAC address, the path is not identified, and an error message appears.
- If the source or destination MAC address belongs to multiple VLANs, you must specify the VLAN to which both the source and destination MAC addresses belong. If the VLAN is not specified, the path is not identified, and an error message appears.
- The `traceroute mac ip` command output shows the Layer 2 path when the specified source and destination IP addresses belong to the same subnet. When you specify the IP addresses, the switch uses the Address Resolution Protocol (ARP) to associate the IP addresses with the corresponding MAC addresses and the VLAN IDs.
  - If an ARP entry exists for the specified IP address, the switch uses the associated MAC address and identifies the physical path.
  - If an ARP entry does not exist, the switch sends an ARP query and tries to resolve the IP address. If the IP address is not resolved, the path is not identified, and an error message appears.
- When multiple devices are attached to one port through hubs (for example, multiple CDP neighbors are detected on a port), the Layer 2 traceroute feature is not supported. When more than one CDP neighbor is detected on a port, the Layer 2 path is not identified, and an error message appears.
- This feature is not supported in Token Ring VLANs.

### Displaying the Physical Path

You can display the physical path that a packet takes from a source device to a destination device by using one of these privileged EXEC commands:

- `tracetroute mac [interface interface-id] {source-mac-address} [interface interface-id] {destination-mac-address} [vlan vlan-id [detail]]`
- `tracetroute mac ip {source-ip-address | source-hostname} {destination-ip-address | destination-hostname} [detail]`

For more information, see the command reference for this release.

### Using IP Traceroute

This section consists of this information:

- Understanding IP Traceroute, page 48-11
- Executing IP Traceroute, page 48-12

### Understanding IP Traceroute

You can use IP traceroute to identify the path that packets take through the network on a hop-by-hop basis. The command output displays all network layer (Layer 3) devices, such as routers, that the traffic passes through on the way to the destination.

Your switches can participate as the source or destination of the `traceroute` privileged EXEC command and might or might not appear as a hop in the `traceroute` command output. If the switch is the destination of the traceroute, it is displayed as the final destination in the traceroute output. Intermediate switches do not show up in the traceroute output if they are only bridging the packet from one port to another within the same VLAN. However, if the intermediate switch is a multilayer switch that is routing a particular packet, this switch shows up as a hop in the traceroute output.

The `traceroute` privileged EXEC command uses the Time To Live (TTL) field in the IP header to cause routers and servers to generate specific return messages. Traceroute starts by sending a User Datagram Protocol (UDP) datagram to the destination host with the TTL field set to 1. If a router finds a TTL value of 1 or 0, it drops the datagram and sends back an Internet Control Message Protocol (ICMP) time-to-live-exceeded message to the sender. Traceroute determines the address of the first hop by examining the source address field of the ICMP time-to-live-exceeded message.

To identify the next hop, traceroute sends a UDP packet with a TTL value of 2. The first router decrements the TTL field by 1 and sends the datagram to the next router. The second router sees a TTL value of 1, discards the datagram, and returns the time-to-live-exceeded message to the source. This process continues until the TTL is incremented to a value large enough for the datagram to reach the destination host (or until the maximum TTL is reached).
To determine when a datagram reaches its destination, traceroute sets the UDP destination port number in the datagram to a very large value that the destination host is unlikely to be using. When a host receives a datagram destined to itself containing a destination port number that is unused locally, it sends an ICMP port unreachable error to the source. Because all errors except port unreachable errors come from intermediate hops, the receipt of a port unreachable error means this message was sent by the destination.

**Executing IP Traceroute**

Beginning in privileged EXEC mode, follow this step to trace the path packets take through the network:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>traceroute ip host</td>
<td>Trace the path packets take through the network by using IP.</td>
</tr>
</tbody>
</table>

**Note**

Though other protocol keywords are available with the `traceroute` privileged EXEC command, they are not supported in this release.

This example shows how to perform a `traceroute` to an IP host:

```
Switch# traceroute ip 171.9.15.10
```

Type escape sequence to abort.
Tracing the route to 171.69.115.10

```
1 172.2.52.1 0 msec 0 msec 4 msec
2 172.2.1.203 12 msec 8 msec 0 msec
3 171.9.16.6 4 msec 0 msec 0 msec
4 171.9.4.5 0 msec 4 msec 0 msec
5 171.9.121.34 0 msec 4 msec 4 msec
6 171.9.15.9 120 msec 132 msec 128 msec
7 171.9.15.10 132 msec 128 msec 128 msec
```

Switch#

The display shows the hop count, IP address of the router, and the round-trip time in milliseconds for each of the three probes that are sent.

**Table 48-2 Traceroute Output Display Characters**

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>The probe timed out.</td>
</tr>
<tr>
<td>?</td>
<td>Unknown packet type.</td>
</tr>
<tr>
<td>A</td>
<td>Administratively unreachable. Usually, this output means that an access list is blocking traffic.</td>
</tr>
<tr>
<td>H</td>
<td>Host unreachable.</td>
</tr>
<tr>
<td>N</td>
<td>Network unreachable.</td>
</tr>
<tr>
<td>P</td>
<td>Protocol unreachable.</td>
</tr>
<tr>
<td>Q</td>
<td>Source quench.</td>
</tr>
<tr>
<td>U</td>
<td>Port unreachable.</td>
</tr>
</tbody>
</table>
To terminate a trace in progress, enter the escape sequence (**Ctrl-^ X** by default). You enter the default by simultaneously pressing and releasing the **Ctrl, Shift, and 6** keys, and then pressing the **X** key.

### Using Debug Commands

This section explains how you use **debug** commands to diagnose and resolve internetworking problems. It contains this information:

- Enabling Debugging on a Specific Feature, page 48-13
- Enabling All-System Diagnostics, page 48-14
- Redirecting Debug and Error Message Output, page 48-14

#### Caution

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. It is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

#### Note

For complete syntax and usage information for specific **debug** commands, see the command reference for this release.

### Enabling Debugging on a Specific Feature

All **debug** commands are entered in privileged EXEC mode, and most **debug** commands take no arguments. For example, beginning in privileged EXEC mode, enter this command to enable the debugging for Switched Port Analyzer (SPAN):

```
Switch# debug span-session
```

The switch continues to generate output until you enter the **no** form of the command.

If you enable a **debug** command and no output appears, consider these possibilities:

- The switch might not be properly configured to generate the type of traffic you want to monitor. Use the **show running-config** command to check its configuration.
- Even if the switch is properly configured, it might not generate the type of traffic you want to monitor during the particular period that debugging is enabled. Depending on the feature you are debugging, you can use commands such as the TCP/IP **ping** command to generate network traffic.

To disable debugging of SPAN, enter this command in privileged EXEC mode:

```
Switch# no debug span-session
```

Alternately, in privileged EXEC mode, you can enter the **undebug** form of the command:

```
Switch# undebug span-session
```

To display the state of each debugging option, enter this command in privileged EXEC mode:

```
Switch# show debugging
```
Enabling All-System Diagnostics

Beginning in privileged EXEC mode, enter this command to enable all-system diagnostics:

```
Switch# debug all
```

---

**Caution**

Because debugging output takes priority over other network traffic, and because the `debug all` privileged EXEC command generates more output than any other `debug` command, it can severely diminish switch performance or even render it unusable. In virtually all cases, it is best to use more specific `debug` commands.

The `no debug all` privileged EXEC command disables all diagnostic output. Using the `no debug all` command is a convenient way to ensure that you have not accidentally left any `debug` commands enabled.

Redirecting Debug and Error Message Output

By default, the network server sends the output from `debug` commands and system error messages to the console. If you use this default, you can use a virtual terminal connection to monitor debug output instead of connecting to the console port.

Possible destinations include the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server. The syslog format is compatible with 4.3 Berkeley Standard Distribution (BSD) UNIX and its derivatives.

---

**Note**

Be aware that the debugging destination you use affects system overhead. Logging messages to the console produces very high overhead, whereas logging messages to a virtual terminal produces less overhead. Logging messages to a syslog server produces even less, and logging to an internal buffer produces the least overhead of any method.

For more information about system message logging, see Chapter 30, “Configuring System Message Logging.”

Using the `show platform forward` Command

The output from the `show platform forward` privileged EXEC command provides some useful information about the forwarding results if a packet entering an interface is sent through the system. Depending upon the parameters entered about the packet, the output provides lookup table results and port maps used to calculate forwarding destinations, bitmaps, and egress information.

---

**Note**

For more syntax and usage information for the `show platform forward` command, see the switch command reference for this release.

Most of the information in the output from the command is useful mainly for technical support personnel, who have access to detailed information about the switch application-specific integrated circuits (ASICs). However, packet forwarding information can also be helpful in troubleshooting.
This is an example of the output from the `show platform forward` command on enhanced-services (ES) port 1 in VLAN 5 when the packet entering that port is addressed to unknown MAC addresses. The packet should be flooded to all other ports in VLAN 5.

```
Switch: show platform forward gigabitethernet1/1 vlan 10 1.1.1 2.2.2 ip 172.18.18.3 172.18.18.1 udp 10 20
Global Port Number:472, Asic Number:1
Src Real Vlan Id:10, Mapped Vlan Id:2
```

**Ingress:**

<table>
<thead>
<tr>
<th>Lookup</th>
<th>Key-Used</th>
<th>Index-Hit</th>
<th>A-Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>InptACL</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>L2Local</td>
<td>80_00020002_00020002-00_00000000_00000000</td>
<td>01850</td>
<td>0000003A</td>
</tr>
<tr>
<td>Station Descriptor:02D30000, DestIndex:02D5, RewriteIndex:F002</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

```
Switch:
show platform forward gigabitethernet1/1 vlan 10 1.1.1 2.2.2 ip 172.18.18.3 172.18.18.1 udp 10 20
Global Port Number:472, Asic Number:1
Src Real Vlan Id:10, Mapped Vlan Id:2
```

**Egress:** Asic 0, switch 1

```
Packet 1
Packet dropped due to failed DEJA_VU Check on Gi1/1/1
```

**Packet 1**

<table>
<thead>
<tr>
<th>Lookup</th>
<th>Key-Used</th>
<th>Index-Hit</th>
<th>A-Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>OutptACL</td>
<td>50_AC121201_AC121203-00_40000014_000A0000</td>
<td>01FFE</td>
<td>0300000</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Vlan</th>
<th>SrcMac</th>
<th>DstMac</th>
<th>Cos</th>
<th>Dscp</th>
<th>Dscp</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>0010</td>
<td>0001.0001.0001</td>
<td>0002.0002.0002</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This is an example of the output from the `show platform forward` command on enhanced-services (ES) port 1 in VLAN 5 when the packet coming in on ES port 1 in VLAN 5 is sent to an address already learned on the VLAN on another port. It should be forwarded from the port on which the address was learned.

```
Switch: show platform forward gigabitethernet1/1 vlan 5 1.1.1 0009.43a8.0145 ip 13.1.1.1 13.2.2.2 udp 10 20
Global Port Number:472, Asic Number:1
Src Real Vlan Id:5, Mapped Vlan Id:5
```

**Ingress:**

<table>
<thead>
<tr>
<th>Lookup</th>
<th>Key-Used</th>
<th>Index-Hit</th>
<th>A-Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>OutptACL</td>
<td>50_AC121201_AC121203-00_40000014_000A0000</td>
<td>01FFE</td>
<td>0300000</td>
</tr>
</tbody>
</table>

```
Packet dropped due to failed DEJA_VU Check on Gi1/1/1
```

This is an example of the output when the packet coming in on ES port 1 in VLAN 5 is sent to an address already learned on the VLAN on another port. It should be forwarded from the port on which the address was learned.
Using the show platform forward Command

This is an example of the output when the packet coming in on ES port 1 in VLAN 5 has a destination MAC address set to the router MAC address in VLAN 5 and the destination IP address unknown. Since there is no default route set, the packet should be dropped.

Switch# show platform forward gigabitethernet1/1/1 vlan 5 1.1.1 03.e319.ee44 ip 13.1.1.1 13.2.2.2 udp 10 20
Global Port Number:472, Asic Number:1
Src Real Vlan Id:5, Mapped Vlan Id:5

This is an example of the output when the packet coming in on ES port 1 in VLAN 5 has a destination MAC address set to the router MAC address in VLAN 5 and the destination IP address set to an IP address that is in the IP routing table. It should be forwarded as specified in the routing table.

Switch# show platform forward gigabitethernet1/1/1 vlan 5 1.1.1 03.e319.ee44 ip 110.1.5.5 16.1.10.5
Global Port Number:472, Asic Number:1
Src Real Vlan Id:5, Mapped Vlan Id:5

This is an example of the output when the packet coming in on ES port 1 in VLAN 5 has a destination MAC address set to the router MAC address in VLAN 5 and the destination IP address set to an IP address that is in the IP routing table. It should be forwarded as specified in the routing table.
Using the crashinfo File

The crashinfo file saves information that helps Cisco technical support representatives to debug problems that caused the Cisco IOS image to fail (crash). The switch writes the crash information to the console at the time of the failure, and the file is created the next time you boot the Cisco IOS image after the failure (instead of while the system is failing).

The information in the file includes the Cisco IOS image name and version that failed, a list of the processor registers, and a stack trace. You can provide this information to the Cisco technical support representative by using the `show tech-support` privileged EXEC command.

All crashinfo files are kept in this directory on the Flash file system:

```
flash:/crashinfo/crashinfo_\n
```

where \n is a sequence number.

Each new crashinfo file that is created uses a sequence number that is larger than any previously-existing sequence number, so the file with the largest sequence number describes the most recent failure. Version numbers are used instead of a timestamp because the switches do not include a real-time clock. You cannot change the name of the file that the system will use when it creates the file. However, after the file is created, you can use the `rename` privileged EXEC command to rename it, but the contents of the renamed file will not be displayed by the `show stacks` or the `show tech-support` privileged EXEC command. You can delete crashinfo files by using the `delete` privileged EXEC command.

You can display the most recent crashinfo file (that is, the file with the highest sequence number at the end of its filename) by entering the `show stacks` or the `show tech-support` privileged EXEC command. You also can access the file by using any command that can copy or display files, such as the `more` or the `copy` privileged EXEC command.

Troubleshooting CPU Utilization

This section lists some possible symptoms that could be caused by the CPU being too busy and shows how to verify a CPU utilization problem. Table 48-3 lists the primary types of CPU utilization problems that you can identify. It gives possible causes and corrective action with links to the Troubleshooting High CPU Utilization document on Cisco.com.

Possible Symptoms of High CPU Utilization

Note that excessive CPU utilization might result in these symptoms, but the symptoms could also result from other causes.

- Spanning tree topology changes
- EtherChannel links brought down due to loss of communication
- Failure to respond to management requests (ICMP ping, SNMP timeouts, slow Telnet or SSH sessions)
- UDP flapping
- IP SLAs failures because of SLAs responses beyond an acceptable threshold
- DHCP or 802.1x failures if the switch does not forward or respond to requests
Layer 3 switches:
- Dropped packets or increased latency for packets routed in software
- BGP or OSPF routing topology changes
- HSRP flapping

Verifying the Problem and Cause

To determine if high CPU utilization is a problem, enter the `show processes cpu sorted` privileged EXEC command. Note the underlined information in the first line of the output example.

```
Switch# show processes cpu sorted
CPU utilization for five seconds: 8%/0%; one minute: 7%; five minutes: 8%
PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process
309 42289103 752750 56180 1.75% 1.20% 1.22% 0 RIP Timers
140 8820183 4942081 1784 0.63% 0.37% 0.30% 0 HRPC qos request
100 3427318 16150534 212 0.47% 0.14% 0.11% 0 HRPC pm-counters
192 3093252 14081112 219 0.31% 0.14% 0.11% 0 Spanning Tree
143 8 37 216 0.15% 0.01% 0.00% 0 Exec
... <output truncated>
```

This example shows normal CPU utilization. The output shows that utilization for the last 5 seconds is 8%/0%, which has this meaning:
- The total CPU utilization is 8 percent, including both time running Cisco IOS processes and time spent handling interrupts.
- The time spent handling interrupts is zero percent.

<table>
<thead>
<tr>
<th>Type of Problem</th>
<th>Cause</th>
<th>Corrective Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interrupt percentage value is almost as high as total CPU utilization value.</td>
<td>The CPU is receiving too many packets from the network.</td>
<td>Determine the source of the network packet. Stop the flow, or change the switch configuration. See the section on “Analyzing Network Traffic.”</td>
</tr>
<tr>
<td>Total CPU utilization is greater than 50% with minimal time spent on interrupts.</td>
<td>One or more Cisco IOS process is consuming too much CPU time. This is usually triggered by an event that activated the process.</td>
<td>Identify the unusual event, and troubleshoot the root cause. See the section on “Debugging Active Processes.”</td>
</tr>
</tbody>
</table>

For complete information about CPU utilization and how to troubleshoot utilization problems, see the Troubleshooting High CPU Utilization document on Cisco.com.
Supported MIBs

This appendix lists the supported MIBs for this release on the Catalyst 3750 Metro switch. It contains these sections:

- MIB List, page A-1
- Using FTP to Access the MIB Files, page A-4

**MIB List**

- **BRIDGE-MIB (RFC1493)**
  
  The BRIDGE-MIB supports the context of a single VLAN. By default, SNMP messages using the configured community string always provide information for VLAN 1. To obtain the BRIDGE-MIB information for other VLANs, for example VLAN x, use this community string in the SNMP message: configured community string @x.

- **CFM MIB**
  

- **CISCO-CABLE-DIAG-MIB**
- **CISCO-CDP-MIB**
- **CISCO-CLASS-BASED-QOS-MIB**
- **CISCO-CLUSTER-MIB**
- **CISCO-CONFIG-COPY-MIB**
- **CISCO-CONFIG-MAN-MIB**
- **CISCO-DHCP-SNOOPING-MIB**
- **CISCO-ENTITY-FRU-CONTROL-MIB**
- **CISCO-ENVMON-MIB**
- CISCO-ETHER-CFM-MIB
- CISCO-FLASH-MIB (Flash memory on all switches is modeled as removable Flash memory.)
- CISCO-FTP-CLIENT-MIB
- CISCO-HSRP-MIB
- CISCO-HSRP-EXT-MIB (partial support)
- CISCO-IETF-PW-MIB
- CISCO-IGMP-FILTER-MIB
- CISCO-IMAGE-MIB
- CISCO-IPS-LA-ETHERNET-MIB
- CISCO-L2L3-INTERFACE-MIB
- CISCO-MAC-NOTIFICATION-MIB
- CISCO-MEMORY-POOL-MIB
- CISCO-NAC-NAD-MIB
- CISCO-PAE-MIB
- CISCO-PAGP-MIB
- CISCO-PING-MIB
- CISCO-PORT-QOS-MIB (the cportQosStats Table returns the values from the octets and packet counters, depending on switch configuration)
- CISCO-PROCESS-MIB

Note: Cisco IOS Release 12.2(37)SE adds CLI support for the cpmCPUThresholdTable objects.

- CISCO-RTTMON-MIB
- CISCO-STACKMAKER-MIB
- CISCO-STP-EXTENSIONS-MIB
- CISCO-SYSLOG-MIB
- CISCO-TCP-MIB
- CISCO-UDLD-MIB
- CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB
- CISCO-VLAN-MEMBERSHIP-MIB
- CISCO-VTP-MIB
- ENTITY-MIB
- ETHERLIKE_MIB
- EXTENDED-BRIDGE-MIB
- IEEE8021-PAE-MIB
- IEEE8023-LACP-MIB
- IF-MIB (In and out counters for VLANs are not supported.)
- IGMP-MIB
Chapter A  Supported MIBs

MIB List

- IPMROUTE-MIB
- MPLS-LDP-MIB
- MPLS-LSR-MIB
- MPLS-VPN-MIB
- OLD-CISCO-CHASSIS-MIB
- OLD-CISCO-FLASH-MIB
- OLD-CISCO-INTERFACES-MIB
- OLD-CISCO-IP-MIB
- OLD-CISCO-SYS-MIB
- OLD-CISCO-TCP-MIB
- OLD-CISCO-TS-MIB
- PIM-MIB
- RFC1213-MIB (Functionality is as per the agent capabilities specified in the CISCO-RFC1213-CAPABILITY.my.)
- RFC1253-MIB (OSPF-MIB)
- RMON-MIB
- RMON2-MIB
- SNMP-FRAMEWORK-MIB
- SNMP-MPD-MIB
- SNMP-NOTIFICATION-MIB
- SNMP-TARGET-MIB
- SNMPv2-MIB
- TCP-MIB
- UDP-MIB

The IEEE-compliant CFM MIB (IEEE CFM MIB) provides MIB support for IEEE 802.1ag compliant CFM (IEEE CFM) services. The IEEE CFM MIB can be used as a tool to trace paths, verify and manage connectivity, and detect faults in a network.

For information about the IEEE CFM MIB and the services it supports, see this URL:

Note

For information about MIB support for a specific Cisco product and release, go to the MIB Locator tool at this URL:
http://tools.cisco.com/ITDIT/MIBS/MainServlet
Using FTP to Access the MIB Files

You can get each MIB file by using this procedure:

Step 1  Make sure that your FTP client is in passive mode.

Note Some FTP clients do not support passive mode.

Step 2  Use FTP to access the server ftp.cisco.com.
Step 3  Log in with the username anonymous.
Step 4  Enter your e-mail username when prompted for the password.
Step 5  At the ftp> prompt, change directories to /pub/mibs/v1 and /pub/mibs/v2.
Step 6  Use the get MIB_filename command to obtain a copy of the MIB file.
Working with the Cisco IOS File System,
Configuration Files, and Software Images

This appendix describes how to manipulate the Catalyst 3750 Metro switch flash file system, how to copy configuration files, and how to archive (upload and download) software images to a switch.

Note
For complete syntax and usage information for the commands used in this chapter, see the switch command reference for this release and the Cisco IOS Configuration Fundamentals Command Reference, Release 12.2.

This appendix consists of these sections:

- Working with the Flash File System, page B-1
- Working with Configuration Files, page B-7
- Replacing and Rolling Back Configurations, page B-18

Working with the Flash File System

The flash file system is a single flash device on which you can store files. It also provides several commands to help you manage software image and configuration files. The default flash file system on the switch is named flash:

This section contains this information:

- Displaying Available File Systems, page B-2
- Setting the Default File System, page B-3
- Displaying Information about Files on a File System, page B-3
- Creating and Removing Directories, page B-4
- Copying Files, page B-4
- Deleting Files, page B-5
- Creating, Displaying, and Extracting tar Files, page B-5
- Displaying the Contents of a File, page B-7
Chapter B: Working with the Cisco IOS File System, Configuration Files, and Software Images

Displaying Available File Systems

To display the available file systems on your switch, use the `show file systems` privileged EXEC command as shown in this example.

```
Switch# show file systems
File Systems:
Size(b) Free(b) Type Flags Prefixes
  * 15998976 5135872 flash rw flash:
    -          - opaque rw bs:
    -          - opaque rw vb:
524288 520138 nvramp rw nvramp:
    -          - network rw tftp:
    -          - opaque rw null:
    -          - opaque rw system:
    -          - opaque ro xmodem:
    -          - opaque ro ymodem:
```

**Table B-1 show file systems Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size(b)</td>
<td>Amount of memory in the file system in bytes.</td>
</tr>
<tr>
<td>Free(b)</td>
<td>Amount of free memory in the file system in bytes.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of file system.</td>
</tr>
<tr>
<td></td>
<td><strong>flash</strong>—The file system is for a flash memory device.</td>
</tr>
<tr>
<td></td>
<td><strong>nvram</strong>—The file system is for a NVRAM device.</td>
</tr>
<tr>
<td></td>
<td><strong>opaque</strong>—The file system is a locally generated <em>pseudo</em> file system (for example, the <em>system</em>) or a download interface, such as brimux.</td>
</tr>
<tr>
<td></td>
<td><strong>unknown</strong>—The file system is an unknown type.</td>
</tr>
<tr>
<td>Flags</td>
<td>Permission for file system.</td>
</tr>
<tr>
<td></td>
<td><strong>ro</strong>—read-only.</td>
</tr>
<tr>
<td></td>
<td><strong>rw</strong>—read/write.</td>
</tr>
<tr>
<td></td>
<td><strong>wo</strong>—write-only.</td>
</tr>
<tr>
<td>Prefixes</td>
<td>Alias for file system.</td>
</tr>
<tr>
<td></td>
<td><strong>flash</strong>—Flash file system.</td>
</tr>
<tr>
<td></td>
<td><strong>nvramp</strong>—NVRAM.</td>
</tr>
<tr>
<td></td>
<td><strong>null</strong>—Null destination for copies. You can copy a remote file to null to find its size.</td>
</tr>
<tr>
<td></td>
<td><strong>rcp</strong>—Remote copy (RCP) network server.</td>
</tr>
<tr>
<td></td>
<td><strong>system</strong>—Contains the system memory, including the running configuration.</td>
</tr>
<tr>
<td></td>
<td><strong>tftp</strong>—TFTP network server.</td>
</tr>
<tr>
<td></td>
<td><strong>xmodem</strong>—Obtain the file from a network machine by using the Xmodem protocol.</td>
</tr>
<tr>
<td></td>
<td><strong>ymodem</strong>—Obtain the file from a network machine by using the Ymodem protocol.</td>
</tr>
</tbody>
</table>
Setting the Default File System

You can specify the file system or directory that the system uses as the default file system by using the `cd filesystem:` privileged EXEC command. You can set the default file system to omit the `filesystem:` argument from related commands. For example, for all privileged EXEC commands that have the optional `filesystem:` argument, the system uses the file system specified by the `cd` command.

By default, the default file system is `flash:`.

You can display the current default file system as specified by the `cd` command by using the `pwd` privileged EXEC command.

Displaying Information about Files on a File System

You can view a list of the contents of a file system before manipulating its contents. For example, before copying a new configuration file to flash memory, you might want to verify that the file system does not already contain a configuration file with the same name. Similarly, before copying a flash configuration file to another location, you might want to verify its filename for use in another command.

To display information about files on a file system, use one of the privileged EXEC commands in Table B-2:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dir [/all] [filesystem:][filename]</code></td>
<td>Display a list of files on a file system.</td>
</tr>
<tr>
<td><code>show file systems</code></td>
<td>Display more information about each of the files on a file system.</td>
</tr>
<tr>
<td><code>show file information file-url</code></td>
<td>Display information about a specific file.</td>
</tr>
<tr>
<td><code>show file descriptors</code></td>
<td>Display a list of open file descriptors. File descriptors are the internal representations of open files. You can use this command to see if another user has a file open.</td>
</tr>
</tbody>
</table>

Changing Directories and Displaying the Working Directory

Beginning in privileged EXEC mode, follow these steps to change directories and display the working directory.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>dir filesystem:</code> Display the directories on the specified file system. For <code>filesystem:</code> use <code>flash:</code> for the system board flash device.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>cd new_configs</code> Change to the directory of interest. The command example shows how to change to the directory named <code>new_configs</code>.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>pwd</code> Display the working directory.</td>
</tr>
</tbody>
</table>
Creating and Removing Directories

Beginning in privileged EXEC mode, follow these steps to create and remove a directory:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>dir filesystem: Display the directories on the specified file system. For filesystem:, use flash: for the system board flash device.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>mkdir old_configs Create a new directory. The command example shows how to create the directory named old_configs. Directory names are case sensitive. Directory names are limited to 45 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>dir filesystem: Verify your entry.</td>
</tr>
</tbody>
</table>

To delete a directory with all its files and subdirectories, use the delete /force /recursive filesystem:file-url privileged EXEC command.

Use the /recursive keyword to delete the named directory and all subdirectories and the files contained in it. Use the /force keyword to suppress the prompting that confirms a deletion of each file in the directory. You are prompted only once at the beginning of this deletion process. Use the /force and /recursive keywords for deleting old software images that were installed by using the archive download-sw command but are no longer needed.

For filesystem, use flash: for the system board flash device. For file-url, enter the name of the directory to be deleted. All the files in the directory and the directory are removed.

**Caution**
When files and directories are deleted, their contents cannot be recovered.

Copying Files

To copy a file from a source to a destination, use the copy source-url destination-url privileged EXEC command. For the source and destination URLs, you can use running-config and startup-config keyword shortcuts. For example, the copy running-config startup-config command saves the currently running configuration file to the NVRAM section of flash memory to be used as the configuration during system initialization.

You can also copy from special file systems (xmodem:, ymodem:) as the source for the file from a network machine that uses the Xmodem or Ymodem protocol.

Network file system URLs include ftp:, rcp:, and tftp: and have these syntaxes:

- FTP—ftp:[][//username [password]@location]directory]filename
- RCP—rcp:[][][//username@location]directory]filename
- TFTP—tftp:[][//location]directory]filename

Local writable file systems include flash:. 

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>dir filesystem:</td>
<td>Display the directories on the specified file system. For filesystem:, use flash: for the system board flash device.</td>
</tr>
<tr>
<td>mkdir old_configs</td>
<td>Create a new directory. The command example shows how to create the directory named old_configs. Directory names are case sensitive. Directory names are limited to 45 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.</td>
</tr>
<tr>
<td>dir filesystem:</td>
<td>Verify your entry.</td>
</tr>
</tbody>
</table>
Some invalid combinations of source and destination exist. Specifically, you cannot copy these combinations:
- From a running configuration to a running configuration
- From a startup configuration to a startup configuration
- From a device to the same device (for example, the `copy flash: flash:` command is invalid)

For specific examples of using the `copy` command with configuration files, see the “Working with Configuration Files” section on page B-7.

To copy software images either by downloading a new version or uploading the existing one, use the `archive download-sw` or the `archive upload-sw` privileged EXEC command. For more information, see the “Replacing and Rolling Back Configurations” section on page B-18.

### Deleting Files

When you no longer need a file on a flash memory device, you can permanently delete it. To delete a file or directory from a specified flash device, use the `delete [force] [recursive] filesystem:/file-url` privileged EXEC command.

Use the `recursive` keyword for deleting a directory and all subdirectories and the files contained in it. Use the `force` keyword to suppress the prompting that confirms a deletion of each file in the directory. You are prompted only once at the beginning of this deletion process. Use the `force` and `recursive` keywords for deleting old software images that were installed by using the `archive download-sw` command but are no longer needed.

If you omit the `filesystem:` option, the switch uses the default device specified by the `cd` command. For `file-url`, you specify the path (directory) and the name of the file to be deleted.

When you attempt to delete any files, the system prompts you to confirm the deletion.

**Caution**

When files are deleted, their contents cannot be recovered.

This example shows how to delete the file `myconfig` from the default flash memory device:

```
Switch# delete myconfig
```

### Creating, Displaying, and Extracting tar Files

You can create a tar file and write files into it, list the files in a tar file, and extract the files from a tar file as described in the next sections.

**Note**

Instead of using the `copy` privileged EXEC command or the `archive tar` privileged EXEC command, we recommend using the `archive download-sw` and `archive upload-sw` privileged EXEC commands to download and upload software image files.

### Creating a tar File

To create a tar file and write files into it, use this privileged EXEC command:

```
archive tar /create destination-url flash:/file-url
```
For destination-url, specify the destination URL alias for the local or network file system and the name of the tar file to create. These options are supported:

- For the local flash file system, the syntax is `flash:`
- For the FTP, the syntax is `ftp://[[username[:password]@location]/directory]/tar-filename.tar`
- For the RCP, the syntax is `rcp://[[username@location]/directory]/tar-filename.tar`
- For the TFTP, the syntax is `tftp://[[location]/directory]/tar-filename.tar`

The `tar-filename.tar` is the tar file to be created.

For flash://file-url, specify the location on the local flash file system from which the new tar file is created. You can also specify an optional list of files or directories within the source directory to write to the new tar file. If none are specified, all files and directories at this level are written to the newly created tar file.

This example shows how to create a tar file. This command writes the contents of the new-configs directory on the local flash device to a file named `saved.tar` on the TFTP server at 172.20.10.30:

```
Switch# archive tar /create tftp:172.20.10.30/saved.tar flash:/new-configs
```

### Displaying the Contents of a Tar File

To display the contents of a tar file on the screen, use this privileged EXEC command:

```
archive tar /table source-url
```

For source-url, specify the source URL alias for the local or network file system. These options are supported:

- For the local flash file system, the syntax is `flash:`
- For the FTP, the syntax is `ftp://[[username[:password]@location]/directory]/tar-filename.tar`
- For the RCP, the syntax is `rcp://[[username@location]/directory]/tar-filename.tar`
- For the TFTP, the syntax is `tftp://[[location]/directory]/tar-filename.tar`

The `tar-filename.tar` is the tar file to display.

You can also limit the display of the files by specifying an optional list of files or directories after the tar file; then only those files appear. If none are specified, all files and directories appear.

This example shows how to display the contents of a switch tar file that is in flash memory:

```
Switch# archive tar /table flash:image-tv0-m.tar
info (219 bytes)
image-tv0-mz-121/ (directory)
image-tv0-mz-121/html/ (directory)
image-tv0-mz-121/html/foo.html (0 bytes)
image-tv0-mz-121/image-tv0-mz-121.bin (610856 bytes)
image-tv0-mz-121/info (219 bytes)
info.ver (219 bytes)
```

This example shows how to display only the `image-tv0-mz-121/html` directory and its contents:

```
Switch# archive tar /table flash:image-tv0-m.tar image-tv0-mz-121/html
image-tv0-mz-121/html/ (directory)
image-tv0-mz-121/html/foo.html (0 bytes)
```
Extracting a tar File

To extract a tar file into a directory on the flash file system, use this privileged EXEC command:

```
archive tar /xtract source-url flash:/file-url [dir/file...]
```

For `source-url`, specify the source URL alias for the local file system. These options are supported:

- For the local flash file system, the syntax is `flash:`
- For the FTP, the syntax is `ftp://[username[:password]@location]/directory]/tar-filename.tar`
- For the RCP, the syntax is `rcp://[username@location]/directory]/tar-filename.tar`
- For the TFTP, the syntax is `tftp://[location]/directory]/tar-filename.tar`

The `tar-filename.tar` is the tar file from which to extract files.

For `flash:/file-url [dir/file...]`, specify the location on the local flash file system into which the tar file is extracted. Use the `dir/file...` option to specify an optional list of files or directories within the tar file to be extracted. If none are specified, all files and directories are extracted.

This example shows how to extract the contents of a tar file located on the TFTP server at 172.20.10.30. This command extracts just the `new-configs` directory into the root directory on the local flash file system. The remaining files in the `saved.tar` file are ignored.

```
Switch# archive tar /xtract tftp://172.20.10.30/saved.tar flash:/new-configs
```

Displaying the Contents of a File

To display the contents of any readable file, including a file on a remote file system, use the `more [/ascii | /binary | /ebcdic] file-url` privileged EXEC command:

This example shows how to display the contents of a configuration file on a TFTP server:

```
Switch# more tftp://serverA/hampton/savedconfig
```

```
! Saved configuration on server
! version 11.3
service timestamps log datetime localtime
service linenumber
service udp-small-servers
service pt-vty-logging
!
<output truncated>
```

Working with Configuration Files

This section describes how to create, load, and maintain configuration files.

Configuration files contain commands entered to customize the function of the Cisco IOS software. A way to create a basic configuration file is to use the `setup` program or to enter the `setup` privileged EXEC command. For more information, see Chapter 3, “Assigning the Switch IP Address and Default Gateway.”
You can copy (download) configuration files from a TFTP, FTP, or RCP server to the running configuration or startup configuration of the switch. You might want to perform this for one of these reasons:

- To restore a backed-up configuration file.
- To use the configuration file for another switch. For example, you might add another switch to your network and want it to have a configuration similar to the original switch. By copying the file to the new switch, you can change the relevant parts rather than recreating the whole file.
- To load the same configuration commands on all the switches in your network so that all the switches have similar configurations.

You can copy (upload) configuration files from the switch to a file server by using TFTP, FTP, or RCP. You might perform this task to back up a current configuration file to a server before changing its contents so that you can later restore the original configuration file from the server.

The protocol you use depends on which type of server you are using. The FTP and RCP transport mechanisms provide faster performance and more reliable delivery of data than TFTP. These improvements are possible because FTP and RCP are built on and use the TCP/IP stack, which is connection-oriented.

This section includes this information:

- Guidelines for Creating and Using Configuration Files, page B-8
- Configuration File Types and Location, page B-9
- Creating a Configuration File By Using a Text Editor, page B-9
- Copying Configuration Files By Using TFTP, page B-9
- Copying Configuration Files By Using FTP, page B-11
- Copying Configuration Files By Using RCP, page B-14
- Clearing Configuration Information, page B-17
- Replacing and Rolling Back Configurations, page B-18

Guidelines for Creating and Using Configuration Files

Creating configuration files can aid in your switch configuration. Configuration files can contain some or all of the commands needed to configure one or more switches. For example, you might want to download the same configuration file to several switches that have the same hardware configuration.

Use these guidelines when creating a configuration file:

- We recommend that you connect through the console port for the initial configuration of the switch. If you are accessing the switch through a network connection instead of through a direct connection to the console port, keep in mind that some configuration changes (such as changing the switch IP address or disabling ports) can cause a loss of connectivity to the switch.
- If no password has been set on the switch, we recommend that you set one by using the `enable secret secret-password` global configuration command.

Note

The `copy {ftp: | rcp: | tftp:} system:running-config` privileged EXEC command loads the configuration files on the switch as if you were entering the commands at the command line. The switch does not erase the existing running configuration before adding the commands. If a command in the copied configuration file replaces a command in the existing configuration file, the existing command is erased. For example, if the copied configuration file contains a different IP address in a particular
command than the existing configuration, the IP address in the copied configuration is used. However, some commands in the existing configuration might not be replaced or negated. In this case, the resulting configuration file is a mixture of the existing configuration file and the copied configuration file, with the copied configuration file having precedence.

To restore a configuration file to an exact copy of a file stored on a server, copy the configuration file directly to the startup configuration (by using the `copy {ftp: | rcp: | tftp:} nvram:startup-config` privileged EXEC command), and reload the switch.

**Configuration File Types and Location**

Startup configuration files are used during system startup to configure the software. Running configuration files contain the current configuration of the software. The two configuration files can be different. For example, you might want to change the configuration for a short time period rather than permanently. In this case, you would change the running configuration but not save the configuration by using the `copy running-config startup-config` privileged EXEC command.

The running configuration is saved in DRAM; the startup configuration is stored in the NVRAM section of flash memory.

**Creating a Configuration File By Using a Text Editor**

When creating a configuration file, you must list commands logically so that the system can respond appropriately. This is one method of creating a configuration file:

- **Step 1** Copy an existing configuration from a switch to a server.
  
  For more information, see the “Downloading the Configuration File By Using TFTP” section on page B-10, the “Downloading a Configuration File By Using FTP” section on page B-12, or the “Downloading a Configuration File By Using RCP” section on page B-16.

- **Step 2** Open the configuration file in a text editor, such as vi or emacs on UNIX or Notepad on a PC.

- **Step 3** Extract the portion of the configuration file with the desired commands, and save it in a new file.

- **Step 4** Copy the configuration file to the appropriate server location. For example, copy the file to the TFTP directory on the workstation (usually /tftpboot on a UNIX workstation).

- **Step 5** Make sure the permissions on the file are set to world-read.

**Copying Configuration Files By Using TFTP**

You can configure the switch by using configuration files you create, download from another switch, or download from a TFTP server. You can copy (upload) configuration files to a TFTP server for storage. This section includes this information:

- Preparing to Download or Upload a Configuration File By Using TFTP, page B-10
- Downloading the Configuration File By Using TFTP, page B-10
- Uploading the Configuration File By Using TFTP, page B-11
Preparing to Download or Upload a Configuration File By Using TFTP

Before you begin downloading or uploading a configuration file by using TFTP, do these tasks:

- Ensure that the workstation acting as the TFTP server is properly configured. On a Sun workstation, make sure that the /etc/inetd.conf file contains this line:

  ```bash
  tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd -p -s /tftpboot
  ```

  Make sure that the /etc/services file contains this line:

  ```bash
  tftp 69/udp
  ```

  **Note**
  You must restart the inetd daemon after modifying the /etc/inetd.conf and /etc/services files. To restart the daemon, either stop the inetd process and restart it, or enter a `fastboot` command (on the SunOS 4.x) or a `reboot` command (on Solaris 2.x or SunOS 5.x). For more information on the TFTP daemon, see the documentation for your workstation.

- Ensure that the switch has a route to the TFTP server. The switch and the TFTP server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the TFTP server by using the `ping` command.

- Ensure that the configuration file to be downloaded is in the correct directory on the TFTP server (usually `/tftpboot` on a UNIX workstation).

- For download operations, ensure that the permissions on the file are set correctly. The permission on the file should be world-readable.

- Before uploading the configuration file, you might need to create an empty file on the TFTP server. To create an empty file, enter the `touch filename` command, where `filename` is the name of the file you will use when uploading it to the server.

- During upload operations, if you are overwriting an existing file (including an empty file, if you had to create one) on the server, ensure that the permissions on the file are set correctly. Permissions on the file should be world-writable.

Downloading the Configuration File By Using TFTP

To configure the switch by using a configuration file downloaded from a TFTP server, follow these steps:

**Step 1** Copy the configuration file to the appropriate TFTP directory on the workstation.

**Step 2** Verify that the TFTP server is properly configured by referring to the “Preparing to Download or Upload a Configuration File By Using TFTP” section on page B-10.

**Step 3** Log into the switch through the console port or a Telnet session.

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

Specify the IP address or hostname of the TFTP server and the name of the file to download. Use one of these privileged EXEC commands:

- `copy tftp://[location]/directory[/filename] system:running-config`
- `copy tftp://[location]/directory[/filename] nvram:startup-config`

The configuration file downloads, and the commands are executed as the file is parsed line-by-line.
Working with Configuration Files

This example shows how to configure the software from the file `tokyo-config` at IP address 172.16.2.155:

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

### Uploading the Configuration File By Using TFTP

To upload a configuration file from a switch to a TFTP server for storage, follow these steps:

1. **Step 1** Verify that the TFTP server is properly configured by referring to the “Preparing to Download or Upload a Configuration File By Using TFTP” section on page B-10.
2. **Step 2** Log into the switch through the console port or a Telnet session.
3. **Step 3** Upload the switch configuration to the TFTP server. Specify the IP address or hostname of the TFTP server and the destination filename.

Use one of these privileged EXEC commands:

- `copy system:running-config tftp://[location]/directory/filename`
- `copy nvram:startup-config tftp://[location]/directory/filename`

The file is uploaded to the TFTP server.

This example shows how to upload a configuration file from a switch to a TFTP server:

```
Switch# copy system:running-config tftp://172.16.2.155/tokyo-config
Write file tokyo-config on host 172.16.2.155? [confirm] y
#
Writing tokyo-config!!! [OK]
```

### Copying Configuration Files By Using FTP

You can copy configuration files to or from an FTP server.

The FTP protocol requires a client to send a remote username and password on each FTP request to a server. When you copy a configuration file from the switch to a server by using FTP, the Cisco IOS software sends the first valid username in this list:

- The username specified in the `copy` command if a username is specified.
- The username set by the `ip ftp username username` global configuration command if the command is configured.
- Anonymous.

The switch sends the first valid password in this list:

- The password specified in the `copy` command if a password is specified.
- The password set by the `ip ftp password password` global configuration command if the command is configured.
- The switch forms a password named `username@switchname.domain`. The variable `username` is the username associated with the current session, `switchname` is the configured hostname, and `domain` is the domain of the switch.
The username and password must be associated with an account on the FTP server. If you are writing to the server, the FTP server must be properly configured to accept your FTP write request.

Use the `ip ftp username` and `ip ftp password` commands to specify a username and password for all copies. Include the username in the `copy` command if you want to specify only a username for that copy operation.

If the server has a directory structure, the configuration file is written to or copied from the directory associated with the username on the server. For example, if the configuration file resides in the home directory of a user on the server, specify that user’s name as the remote username.

For more information, see the documentation for your FTP server.

This section includes this information:
- Preparing to Download or Upload a Configuration File By Using FTP, page B-12
- Downloading a Configuration File By Using FTP, page B-12
- Uploading a Configuration File By Using FTP, page B-13

### Preparing to Download or Upload a Configuration File By Using FTP

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

- Ensure that the switch has a route to the FTP server. The switch and the FTP server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the FTP server by using the `ping` command.

- If you are accessing the switch through the console or a Telnet session and you do not have a valid username, make sure that the current FTP username is the one that you want to use for the FTP download. You can enter the `show users` privileged EXEC command to view the valid username. If you do not want to use this username, create a new FTP username by using the `ip ftp username` global configuration command during all copy operations. The new username is stored in NVRAM. If you are accessing the switch through a Telnet session and you have a valid username, this username is used, and you do not need to set the FTP username. Include the username in the `copy` command if you want to specify a username for only that copy operation.

- When you upload a configuration file to the FTP server, it must be properly configured to accept the write request from the user on the switch.

For more information, see the documentation for your FTP server.

### Downloading a Configuration File By Using FTP

Beginning in privileged EXEC mode, follow these steps to download a configuration file by using FTP:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Verify that the FTP server is properly configured by referring to the “Preparing to Download or Upload a Configuration File By Using FTP” section on page B-12.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Log into the switch through the console port or a Telnet session.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode on the switch. This step is required only if you override the default remote username or password (see Steps 4, 5, and 6).</td>
</tr>
</tbody>
</table>
This example shows how to copy a configuration file named `host1-confg` from the `netadmin1` directory on the remote server with an IP address of 172.16.101.101 and to load and run those commands on the switch:

```
Switch# copy ftp://netadmin1:mypass@172.16.101.101/host1-confg system:running-config
```

```
Configure using host1-confg from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-confg:![OK]
```

```
%SYS-5-CONFIG: Configured from host1-config by ftp from 172.16.101.101
```

This example shows how to specify a remote username of `netadmin1`. The software copies the configuration file `host2-confg` from the `netadmin1` directory on the remote server with an IP address of 172.16.101.101 to the switch startup configuration.

```
Switch# configure terminal
Switch(config)# ip ftp username netadmin1
Switch(config)# ip ftp password mypass
Switch(config)# end
Switch# copy ftp: nvram:startup-config
```

```
Address of remote host [255.255.255.255]? 172.16.101.101
Name of configuration file[rtr2-conf?0g] host2-conf?0g
Configure using host2-conf?0g from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-conf:![OK]
```

```
%SYS-5-CONFIG_NV:Non-volatile store configured from host2-config by ftp from 172.16.101.101
```

### Uploading a Configuration File By Using FTP

Beginning in privileged EXEC mode, follow these steps to upload a configuration file by using FTP:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>ip ftp username username</code></td>
<td>(Optional) Change the default remote username.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>ip ftp password password</code></td>
<td>(Optional) Change the default password.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>copy ftp://[username[:password]@]location/directory] [filename] system:running-config</code></td>
<td>Using FTP, copy the configuration file from a network server to the running configuration or to the startup configuration file.</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>copy ftp://[username[:password]@]location/directory] [filename] nvram:startup-config</code></td>
<td></td>
</tr>
</tbody>
</table>

### Command Purpose

**Step 1**

Verify that the FTP server is properly configured by referring to the “Preparing to Download or Upload a Configuration File By Using FTP” section on page B-12.

**Step 2**

Log into the switch through the console port or a Telnet session.
Working with Configuration Files

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 3    | configure terminal | Enter global configuration mode.  
This step is required only if you override the default remote username or password (see Steps 4, 5, and 6). |
| 4    | ip ftp username username | (Optional) Change the default remote username. |
| 5    | ip ftp password password | (Optional) Change the default password. |
| 6    | end | Return to privileged EXEC mode. |
| 7    | copy system:running-config ftp://username:password@location/directory/filename | Using FTP, store the switch running or startup configuration file to the specified location.  
| or | copy nvram:startup-config ftp://username:password@location/directory/filename | |

This example shows how to copy the running configuration file named `switch2-config` to the `netadmin1` directory on the remote host with an IP address of 172.16.101.101:

```plaintext
Switch# copy system:running-config ftp://netadmin1:mypass@172.16.101.101/switch2-config
Write file switch2-config on host 172.16.101.101?[confirm]
Building configuration...[OK]
Connected to 172.16.101.101
Switch#
```

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

```plaintext
Switch# configure terminal
Switch(config)# ip ftp username netadmin2
Switch(config)# ip ftp password mypass
Switch(config)# end
Switch# copy nvram:startup-config ftp://netadmin2:mypass@172.16.101.101/switch2-config
Remote host[?] 172.16.101.101
Name of configuration file to write [switch2-config]? Write file switch2-config on host 172.16.101.101?[confirm] ![OK]
```

Copy Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| configure terminal | Enter global configuration mode.  
This step is required only if you override the default remote username or password (see Steps 4, 5, and 6). |
| ip ftp username username | (Optional) Change the default remote username. |
| ip ftp password password | (Optional) Change the default password. |
| end | Return to privileged EXEC mode. |
| copy system:running-config ftp://username:password@location/directory/filename | Using FTP, store the switch running or startup configuration file to the specified location.  
| or | copy nvram:startup-config ftp://username:password@location/directory/filename | |

Copy Configuration Files By Using RCP

The RCP provides another method of downloading, uploading, and copying configuration files between remote hosts and the switch. Unlike TFTP, which uses User Datagram Protocol (UDP), a connectionless protocol, RCP uses TCP, which is connection-oriented.

To use RCP to copy files, the server from or to which you will be copying files must support RCP. The RCP copy commands rely on the rsh server (or daemon) on the remote system. To copy files by using RCP, you do not need to create a server for file distribution as you do with TFTP. You only need to have access to a server that supports the remote shell (rsh). (Most UNIX systems support rsh.) Because you are copying a file from one place to another, you must have read permission on the source file and write permission on the destination file. If the destination file does not exist, RCP creates it for you.
The RCP requires a client to send a remote username with each RCP request to a server. When you copy a configuration file from the switch to a server, the Cisco IOS software sends the first valid username in this list:

- The username specified in the `copy` command if a username is specified.
- The username set by the `ip rcmd remote-username username` global configuration command if the command is configured.
- The remote username associated with the current TTY (terminal) process. For example, if the user is connected to the router through Telnet and was authenticated through the `username` command, the switch software sends the Telnet username as the remote username.
- The switch hostname.

For a successful RCP copy request, you must define an account on the network server for the remote username. If the server has a directory structure, the configuration file is written to or copied from the directory associated with the remote username on the server. For example, if the configuration file is in the home directory of a user on the server, specify that user's name as the remote username.

This section includes this information:

- Preparing to Download or Upload a Configuration File By Using RCP, page B-15
- Downloading a Configuration File By Using RCP, page B-16
- Uploading a Configuration File By Using RCP, page B-17

Preparing to Download or Upload a Configuration File By Using RCP

Before you begin downloading or uploading a configuration file by using RCP, do these tasks:

- Ensure that the workstation acting as the RCP server supports the remote shell (rsh).
- Ensure that the switch has a route to the RCP server. The switch and the server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the RCP server by using the `ping` command.
- If you are accessing the switch through the console or a Telnet session and you do not have a valid username, make sure that the current RCP username is the one that you want to use for the RCP download. You can enter the `show users` privileged EXEC command to view the valid username. If you do not want to use this username, create a new RCP username by using the `ip rcmd remote-username username` global configuration command to be used during all copy operations. The new username is stored in NVRAM. If you are accessing the switch through a Telnet session and you have a valid username, this username is used, and you do not need to set the RCP username. Include the username in the `copy` command if you want to specify a username for only that copy operation.
- When you upload a file to the RCP server, it must be properly configured to accept the RCP write request from the user on the switch. For UNIX systems, you must add an entry to the .rhosts file for the remote user on the RCP server. For example, suppose that the switch contains these configuration lines:

  ```
  hostname Switch1
  ip rcmd remote-username User0
  ```

  If the switch IP address translates to `Switch1.company.com`, the .rhosts file for User0 on the RCP server should contain this line:

  ```
  Switch1.company.com Switch1
  ```

  For more information, see the documentation for your RCP server.
**Downloading a Configuration File By Using RCP**

Beginning in privileged EXEC mode, follow these steps to download a configuration file by using RCP:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Verify that the RCP server is properly configured by referring to the “Preparing to Download or Upload a Configuration File By Using RCP” section on page B-15.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Log into the switch through the console port or a Telnet session.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Enter global configuration mode. This step is required only if you override the default remote username (see Steps 4 and 5).</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>(Optional) Specify the remote username.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Using RCP, copy the configuration file from a network server to the running configuration or to the startup configuration file.</td>
</tr>
</tbody>
</table>

This example shows how to copy a configuration file named `host1-confg` from the `netadmin1` directory on the remote server with an IP address of 172.16.101.101 and load and run those commands on the switch:

```
Switch# copy rcp://netadmin1@172.16.101.101/host1-confg system:running-config
Configure using host1-confg from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-confg:![OK]
Switch%
%SYS-5-CONFIG: Configured from host1-config by rcp from 172.16.101.101
```

This example shows how to specify a remote username of `netadmin1`. Then it copies the configuration file `host2-confg` from the `netadmin1` directory on the remote server with an IP address of 172.16.101.101 to the startup configuration:

```
Switch# configure terminal
Switch(config)# ip rcmd remote-username netadmin1
Switch(config)# end
Switch# copy rcp://[username@[location]/directory]/filename
Address of remote host [255.255.255.255]? 172.16.101.101
Name of configuration file [rtr2-config]? host2-confg
Configure using host2-confg from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-confg: ![OK]
[OK]
Switch%
%SYS-5-CONFIG_NV:Non-volatile store configured from host2-config by rcp from 172.16.101.101
```
## Uploading a Configuration File By Using RCP

Beginning in privileged EXEC mode, follow these steps to upload a configuration file by using RCP:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>Verify that the RCP server is properly configured by referring to the “Preparing to Download or Upload a Configuration File By Using RCP” section on page B-15.</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>Log into the switch through the console port or a Telnet session.</td>
</tr>
<tr>
<td>3</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>4</td>
<td>ip rcmd remote-username username</td>
<td>(Optional) Specify the remote username.</td>
</tr>
<tr>
<td>5</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>6</td>
<td>copy system:running-config rcp://username@location/directory/filename</td>
<td>Using RCP, copy the configuration file from a switch running or startup configuration file to a network server.</td>
</tr>
<tr>
<td></td>
<td>or copy nvram:startup-config rcp://username@location/directory/filename</td>
<td></td>
</tr>
</tbody>
</table>

This example shows how to copy the running configuration file named `switch2-config` to the `netadmin1` directory on the remote host with an IP address of 172.16.101.101:

```
Switch# copy system:running-config rcp://netadmin1@172.16.101.101/switch2-config
Write file switch-confg on host 172.16.101.101?[confirm]
Building configuration...[OK]
Connected to 172.16.101.101
Switch#
```

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

```
Switch# configure terminal
Switch(config)# ip rcmd remote-username netadmin2
Switch(config)# end
Switch# copy nvram:startup-config rcp:
Remote host[]? 172.16.101.101
Name of configuration file to write [switch2-config]?
Write file switch2-config on host 172.16.101.101?[confirm]
! [OK]
```

## Clearing Configuration Information

You can clear the configuration information from the startup configuration. If you reboot the switch with no startup configuration, the switch enters the setup program so that you can reconfigure the switch with all new settings.
Clearing the Startup Configuration File

To clear the contents of your startup configuration, use the `erase nvram:` or the `erase startup-config` privileged EXEC command.

⚠️ **Caution** You cannot restore the startup configuration file after it has been deleted.

Deleting a Stored Configuration File

To delete a saved configuration from flash memory, use the `delete flash:filename` privileged EXEC command. Depending on the setting of the `file prompt` global configuration command, you might be prompted for confirmation before you delete a file. By default, the switch prompts for confirmation on destructive file operations. For more information about the `file prompt` command, see the *Cisco IOS Command Reference for Release 12.2*.

⚠️ **Caution** You cannot restore a file after it has been deleted.

Replacing and Rolling Back Configurations

The configuration replacement and rollback feature replaces the running configuration with any saved Cisco IOS configuration file. You can use the rollback function to roll back to a previous configuration.

These sections contain this information:

- Understanding Configuration Replacement and Rollback, page B-18
- Configuration Guidelines, page B-19
- Configuring the Configuration Archive, page B-20
- Performing a Configuration Replacement or Rollback Operation, page B-21

Understanding Configuration Replacement and Rollback

To use the configuration replacement and rollback feature, you should understand these concepts:

- Archiving a Configuration, page B-18
- Replacing a Configuration, page B-19
- Rolling Back a Configuration, page B-19

Archiving a Configuration

The configuration archive provides a mechanism to store, organize, and manage an archive of configuration files. The `configure replace` privileged EXEC command increases the configuration rollback capability. As an alternative, you can save copies of the running configuration by using the `copy running-config destination-url` privileged EXEC command, storing the replacement file either locally or remotely. However, this method lacks any automated file management. The configuration replacement and rollback feature can automatically save copies of the running configuration to the configuration archive.
You use the `archive config` privileged EXEC command to save configurations in the configuration archive by using a standard location and filename prefix that is automatically appended with an incremental version number (and optional timestamp) as each consecutive file is saved. You can specify how many versions of the running configuration are kept in the archive. After the maximum number of files are saved, the oldest file is automatically deleted when the next, most recent file is saved. The `show archive` privileged EXEC command displays information for all the configuration files saved in the configuration archive.

The Cisco IOS configuration archive, in which the configuration files are stored and available for use with the `configure replace` command, is in any of these file systems: FTP, HTTP, RCP, TFTP.

**Replacing a Configuration**

The `configure replace` privileged EXEC command replaces the running configuration with any saved configuration file. When you enter the `configure replace` command, the running configuration is compared with the specified replacement configuration, and a set of configuration differences is generated. The resulting differences are used to replace the configuration. The configuration replacement operation is usually completed in no more than three passes. To prevent looping behavior no more than five passes are performed.

You can use the `copy source-url running-config` privileged EXEC command to copy a stored configuration file to the running configuration. When using this command as an alternative to the `configure replace` command, note these major differences:

- The `copy source-url running-config` command is a merge operation and preserves all the commands from both the source file and the running configuration. This command does not remove commands from the running configuration that are not present in the source file. In contrast, the `configure replace target-url` command removes commands from the running configuration that are not present in the replacement file and adds commands to the running configuration that are not present.

- You can use a partial configuration file as the source file for the `copy source-url running-config` command. You must use a complete configuration file as the replacement file for the `configure replace target-url` command.

**Rolling Back a Configuration**

You can also use the `configure replace` command to roll back changes that were made since the previous configuration was saved. Instead of basing the rollback operation on a specific set of changes that were applied, the configuration rollback capability reverts to a specific configuration based on a saved configuration file.

If you want the configuration rollback capability, you must first save the running configuration before making any configuration changes. Then, after entering configuration changes, you can use that saved configuration file to roll back the changes by using the `configure replace target-url` command.

You can specify any saved configuration file as the rollback configuration. You are not limited to a fixed number of rollbacks, as is the case in some rollback models.

**Configuration Guidelines**

Follow these guidelines when configuring and performing configuration replacement and rollback:

- Make sure that the switch has free memory larger than the combined size of the two configuration files (the running configuration and the saved replacement configuration). Otherwise, the configuration replacement operation fails.
• Make sure that the switch also has sufficient free memory to execute the configuration replacement or rollback configuration commands.

• Certain configuration commands, such as those pertaining to physical components of a networking device (for example, physical interfaces), cannot be added or removed from the running configuration.
  
  – A configuration replacement operation cannot remove the `interface interface-id` command line from the running configuration if that interface is physically present on the device.
  
  – The `interface interface-id` command line cannot be added to the running configuration if no such interface is physically present on the device.

• When using the `configure replace` command, you must specify a saved configuration as the replacement configuration file for the running configuration. The replacement file must be a complete configuration generated by a Cisco IOS device (for example, a configuration generated by the `copy running-config destination-url` command).

  **Note** If you generate the replacement configuration file externally, it must comply with the format of files generated by Cisco IOS devices.

### Configuring the Configuration Archive

Using the `configure replace` command with the configuration archive and with the `archive config` command is optional but offers significant benefit for configuration rollback scenarios. Before using the `archive config command`, you must first configure the configuration archive. Starting in privileged EXEC mode, follow these steps to configure the configuration archive:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>archive</code></td>
<td>Enter archive configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>path url</code></td>
<td>Specify the location and filename prefix for the files in the configuration archive.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td><code>maximum number</code></td>
<td>(Optional) Set the maximum number of archive files of the running configuration to be saved in the configuration archive.</td>
</tr>
<tr>
<td><code>number</code></td>
<td>Maximum files of the running configuration file in the configuration archive. Valid values are from 1 to 14. The default is 10.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Before using this command, you must first enter the `path archive configuration command to specify the location and filename prefix for the files in the configuration archive.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td><code>time-period minutes</code></td>
<td>(Optional) Set the time increment for automatically saving an archive file of the running configuration in the configuration archive.</td>
</tr>
<tr>
<td><code>minutes</code></td>
<td>Specify how often, in minutes, to automatically save an archive file of the running configuration in the configuration archive.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td></td>
</tr>
<tr>
<td><code>show running-config</code></td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td></td>
</tr>
<tr>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
Performing a Configuration Replacement or Rollback Operation

Starting in privileged EXEC mode, follow these steps to replace the running configuration file with a saved configuration file:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>archive config</strong></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Enter the <em>path</em> archive configuration command before using this command.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>exit</strong></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>configure replace target-url [list] [force] [time seconds] [nolock]</strong></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>configure confirm</strong></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>copy running-config startup-config</strong></td>
</tr>
</tbody>
</table>
Working with Software Images

This section describes how to archive (download and upload) software image files, which contain the system software and the Cisco IOS code.

Instead of using the copy privileged EXEC command or the archive tar privileged EXEC command, we recommend using the archive download-sw and archive upload-sw privileged EXEC commands to download and upload software image files.

You download a switch image file from a TFTP, FTP, or RCP server to upgrade the switch software. If you do not have access to a TFTP server, you can download a software image file directly to your PC or workstation by using a web browser (HTTP). You can replace the current image with the new one or keep the current image in flash memory after a download.

You upload a switch image file to a TFTP, FTP, or RCP server for backup purposes. You can use this uploaded image for future downloads to the same switch or another of the same type.

The protocol you use depends on which type of server you are using. The FTP and RCP transport mechanisms provide faster performance and more reliable delivery of data than TFTP. These improvements are possible because FTP and RCP are built on and use the TCP/IP stack, which is connection-oriented.

This section includes this information:

- Image Location on the Switch, page B-22
- tar File Format of Images on a Server or Cisco.com, page B-23
- Copying Image Files By Using TFTP, page B-23
- Copying Image Files By Using FTP, page B-26
- Copying Image Files By Using RCP, page B-31

For a list of software images and the supported upgrade paths, see the release notes that shipped with your switch.

Image Location on the Switch

The Cisco IOS image is stored as a .bin file in a directory that shows the version number. The image is stored on the system board flash memory (flash:).

You can use the show version privileged EXEC command to see the software version that is currently running on your switch. In the display, check the line that begins with System image file is.... It shows the directory name in flash memory where the image is stored.

You can also use the dir filesystem: privileged EXEC command to see the directory names of other software images you might have stored in flash memory.
Software images located on a server or downloaded from Cisco.com are provided in a tar file format, which contains these files:

- An *info* file, which serves as a table of contents for the tar file
- One or more subdirectories containing other images and files, such as Cisco IOS images

This example shows some of the information contained in the info file. Table B-3 provides additional details about this information:

```
version_suffix:i5-121.14-AX
version_directory:c3750me-i5-mz.121.14-AX
image_system_type_id:0x00000001
image_name:c3750me-i5-mz.121.14-AX.bin
ios_image_file_size:4782592
total_image_file_size:4784128
image_feature:LAYER_3|MIN_DRAM_MEG=64
image_family:C3750ME
stacking_number:1.1
board_ids:0x00000004
info_end:
```

**Note** Disregard the stacking_number field. It does not apply to the switch.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>version_suffix</td>
<td>Specifies the Cisco IOS image version string suffix</td>
</tr>
<tr>
<td>version_directory</td>
<td>Specifies the directory where the Cisco IOS image is installed</td>
</tr>
<tr>
<td>image_name</td>
<td>Specifies the name of the Cisco IOS image within the tar file</td>
</tr>
<tr>
<td>ios_image_file_size</td>
<td>Specifies the Cisco IOS image size in the tar file, which is an approximate measure of how much flash memory is required to hold just the Cisco IOS image</td>
</tr>
<tr>
<td>total_image_file_size</td>
<td>Specifies the size of all the images (the Cisco IOS image files) in the tar file, which is an approximate measure of how much flash memory is required to hold them</td>
</tr>
<tr>
<td>image_feature</td>
<td>Describes the core functionality of the image</td>
</tr>
<tr>
<td>image_family</td>
<td>Describes the family of products on which the software can be installed</td>
</tr>
</tbody>
</table>

### Copying Image Files By Using TFTP

You can download a switch image from a TFTP server or upload the image from the switch to a TFTP server.

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

You upload a switch image file to a server for backup purposes; this uploaded image can be used for future downloads to the same or another switch of the same type.
Instead of using the **copy** privileged EXEC command or the **archive tar** privileged EXEC command, we recommend using the **archive download-sw** and **archive upload-sw** privileged EXEC commands to download and upload software image files.

This section includes this information:
- Preparing to Download or Upload an Image File By Using TFTP, page B-24
- Downloading an Image File By Using TFTP, page B-25
- Uploading an Image File By Using TFTP, page B-26

### Preparing to Download or Upload an Image File By Using TFTP

Before you begin downloading or uploading an image file by using TFTP, do these tasks:

- Ensure that the workstation acting as the TFTP server is properly configured. On a Sun workstation, make sure that the `/etc/inetd.conf` file contains this line:
  ```bash
  tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd -p -s /tftpboot
  ```
  Make sure that the `/etc/services` file contains this line:
  ```bash
  tftp 69/udp
  ```

  **Note** You must restart the inetd daemon after modifying the `/etc/inetd.conf` and `/etc/services` files. To restart the daemon, either stop the inetd process and restart it, or enter a `fastboot` command (on the SunOS 4.x) or a `reboot` command (on Solaris 2.x or SunOS 5.x). For more information on the TFTP daemon, see the documentation for your workstation.

- Ensure that the switch has a route to the TFTP server. The switch and the TFTP server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the TFTP server by using the `ping` command.
- Ensure that the image to be downloaded is in the correct directory on the TFTP server (usually `/tftpboot` on a UNIX workstation).
- For download operations, ensure that the permissions on the file are set correctly. The permission on the file should be world-read.
- Before uploading the image file, you might need to create an empty file on the TFTP server. To create an empty file, enter the `touch filename` command, where `filename` is the name of the file you will use when uploading the image to the server.
- During upload operations, if you are overwriting an existing file (including an empty file, if you had to create one) on the server, ensure that the permissions on the file are set correctly. Permissions on the file should be world-write.
## Downloading an Image File By Using TFTP

You can download a new image file and replace the current image or keep the current image.

Beginning in privileged EXEC mode, follow Steps 1 through 3 to download a new image from a TFTP server and overwrite the existing image. To keep the current image, go to Step 3.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 Copy the image to the appropriate TFTP directory on the workstation. Make sure the TFTP server is properly configured; see the “Preparing to Download or Upload an Image File By Using TFTP” section on page B-24.</td>
<td></td>
</tr>
<tr>
<td>Step 2 Log into the switch through the console port or a Telnet session.</td>
<td></td>
</tr>
</tbody>
</table>
| Step 3 archive download-sw /overwrite /reload tftp:[//location]/directory/image-name.tar | Download the image file from the TFTP server to the switch, and overwrite the current image.  
  - The /overwrite option overwrites the software image in flash memory with the downloaded image.  
  - The /reload option reloads the system after downloading the image unless the configuration has been changed and not been saved.  
  - For //location, specify the IP address of the TFTP server.  
  - For /directory/image-name.tar, specify the directory (optional) and the image to download. Directory and image names are case sensitive. |
| Step 4 archive download-sw /leave-old-sw /reload tftp:[//location]/directory/image-name.tar | Download the image file from the TFTP server to the switch, and keep the current image.  
  - The /leave-old-sw option keeps the old software version after a download.  
  - The /reload option reloads the system after downloading the image unless the configuration has been changed and not been saved.  
  - For //location, specify the IP address of the TFTP server.  
  - For /directory/image-name.tar, specify the directory (optional) and the image to download. Directory and image names are case sensitive. |

The download algorithm verifies that the image is appropriate for the switch model and that enough DRAM is present, or it aborts the process and reports an error. If you specify the /overwrite option, the download algorithm removes the existing image on the flash device whether or not it is the same as the new one, downloads the new image, and then reloads the software.

### Note
If the flash device has sufficient space to hold two images and you want to overwrite one of these images with the same version, you must specify the /overwrite option.
Working with Software Images

If you specify the `/leave-old-sw`, the existing files are not removed. If there is not enough space to install the new image and keep the current running image, the download process stops, and an error message appears.

The algorithm installs the downloaded image on the system board flash device (flash:). The image is placed into a new directory named with the software version string, and the BOOT environment variable is updated to point to the newly installed image.

If you kept the old image during the download process (you specified the `/leave-old-sw` keyword), you can remove it by entering the `delete /force /recursive filesystem:file-url` privileged EXEC command. For `filesystem`, use `flash:` for the system board flash device. For `file-url`, enter the directory name of the old image. All the files in the directory and the directory are removed.

Caution

For the download and upload algorithms to operate properly, do not rename image names.

Uploading an Image File By Using TFTP

You can upload an image from the switch to a TFTP server. You can later download this image to the switch or to another switch of the same type.

Beginning in privileged EXEC mode, follow these steps to upload an image to a TFTP server:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Make sure the TFTP server is properly configured; see the</td>
</tr>
<tr>
<td></td>
<td>“Preparing to Download or Upload an Image File By Using TFTP” section</td>
</tr>
<tr>
<td></td>
<td>on page B-24.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Log into the switch through the console port or a Telnet session.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>archive upload-sw tftp:[//location]/directory/image-name.tar</code></td>
</tr>
<tr>
<td></td>
<td>Upload the currently running switch image to the TFTP server.</td>
</tr>
<tr>
<td></td>
<td>• For <code>//location</code>, specify the IP address of the TFTP server.</td>
</tr>
<tr>
<td></td>
<td>• For <code>/directory/image-name.tar</code>, specify the directory (optional)</td>
</tr>
<tr>
<td></td>
<td>and the name of the software image to be uploaded. Directory</td>
</tr>
<tr>
<td></td>
<td>and image names are case sensitive. The <code>image-name.tar</code> is the</td>
</tr>
<tr>
<td></td>
<td>name of the software image to be stored on the server.</td>
</tr>
</tbody>
</table>

The `archive upload-sw` privileged EXEC command builds an image file on the server by uploading the info file and the Cisco IOS image file. After these files are uploaded, the upload algorithm creates the tar file format.

Caution

For the download and upload algorithms to operate properly, do not rename image names.

Copying Image Files By Using FTP

You can download a switch image from an FTP server or upload the image from the switch to an FTP server.

You download a switch image file from a server to upgrade the switch software. You can overwrite the current image with the new one or keep the current image after a download.
You upload a switch image file to a server for backup purposes. You can use this uploaded image for future downloads to the switch or another switch of the same type.

Instead of using the copy privileged EXEC command or the archive tar privileged EXEC command, we recommend using the archive download-sw and archive upload-sw privileged EXEC commands to download and upload software image files.

This section includes this information:

- Preparing to Download or Upload an Image File By Using FTP, page B-27
- Downloading an Image File By Using FTP, page B-28
- Uploading an Image File By Using FTP, page B-30

Preparing to Download or Upload an Image File By Using FTP

You can copy image files to or from an FTP server.

The FTP protocol requires a client to send a remote username and password on each FTP request to a server. When you copy an image file from the switch to a server by using FTP, the Cisco IOS software sends the first valid username in this list:

- The username specified in the archive download-sw or archive upload-sw privileged EXEC command if a username is specified.
- The username set by the ip ftp username username global configuration command if the command is configured.
- Anonymous.

The switch sends the first valid password in this list:

- The password specified in the archive download-sw or archive upload-sw privileged EXEC command if a password is specified.
- The password set by the ip ftp password password global configuration command if the command is configured.
- The switch forms a password named username@switchname.domain. The variable username is the username associated with the current session, switchname is the configured hostname, and domain is the domain of the switch.

The username and password must be associated with an account on the FTP server. If you are writing to the server, the FTP server must be properly configured to accept the FTP write request from you.

Use the ip ftp username and ip ftp password commands to specify a username and password for all copies. Include the username in the archive download-sw or archive upload-sw privileged EXEC command if you want to specify a username only for that operation.

If the server has a directory structure, the image file is written to or copied from the directory associated with the username on the server. For example, if the image file resides in the home directory of a user on the server, specify that user's name as the remote username.

Before you begin downloading or uploading an image file by using FTP, do these tasks:

- Ensure that the switch has a route to the FTP server. The switch and the FTP server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the FTP server by using the ping command.
• If you are accessing the switch through the console or a Telnet session and you do not have a valid username, make sure that the current FTP username is the one that you want to use for the FTP download. You can enter the show users privileged EXEC command to view the valid username. If you do not want to use this username, create a new FTP username by using the ip ftp username username global configuration command. This new name will be used during all archive operations. The new username is stored in NVRAM. If you are accessing the switch through a Telnet session and you have a valid username, this username is used, and you do not need to set the FTP username. Include the username in the archive download-sw or archive upload-sw privileged EXEC command if you want to specify a username for that operation only.

• When you upload an image file to the FTP server, it must be properly configured to accept the write request from the user on the switch.

For more information, see the documentation for your FTP server.

**Downloading an Image File By Using FTP**

You can download a new image file and overwrite the current image or keep the current image.

Beginning in privileged EXEC mode, follow Steps 1 through 7 to download a new image from an FTP server and overwrite the existing image. To keep the current image, go to Step 7.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Verify that the FTP server is properly configured by referring to the “Preparing to Download or Upload an Image File By Using FTP” section on page B-27.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Log into the switch through the console port or a Telnet session.</td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode. This step is required only if you override the default remote username or password (see Steps 4, 5, and 6).</td>
</tr>
<tr>
<td>Step 4 ip ftp username username</td>
<td>(Optional) Change the default remote username.</td>
</tr>
<tr>
<td>Step 5 ip ftp password password</td>
<td>(Optional) Change the default password.</td>
</tr>
<tr>
<td>Step 6 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
## Working with Software Images

The download algorithm verifies that the image is appropriate for the switch model and that enough DRAM is present, or it aborts the process and reports an error. If you specify the `/overwrite` option, the download algorithm removes the existing image on the flash device, whether or not it is the same as the new one, downloads the new image, and then reloads the software.

### Note
If the flash device has sufficient space to hold two images and you want to overwrite one of these images with the same version, you must specify the `/overwrite` option.

If you specify the `/leave-old-sw`, the existing files are not removed. If there is not enough space to install the new image and keep the running image, the download process stops, and an error message appears.

### Command Syntax and Purpose

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 7    | `archive download-sw /overwrite /reload ftp://[[Username][:password]@[location]/directory] /image-name.tar` | Download the image file from the FTP server to the switch, and overwrite the current image.  
- The `/overwrite` option overwrites the software image in flash memory with the downloaded image.  
- The `/reload` option reloads the system after downloading the image unless the configuration has been changed and not been saved.  
- For `/Username[:password]`, specify the username and password; these must be associated with an account on the FTP server. For more information, see the “Preparing to Download or Upload an Image File By Using FTP” section on page B-27.  
- For `/location`, specify the IP address of the FTP server.  
- For `/directory/image-name.tar`, specify the directory (optional) and the image to download. Directory and image names are case sensitive. |
| 8    | `archive download-sw /leave-old-sw /reload ftp://[[Username][:password]@[location]/directory] /image-name.tar` | Download the image file from the FTP server to the switch, and keep the current image.  
- The `/leave-old-sw` option keeps the old software version after a download.  
- The `/reload` option reloads the system after downloading the image unless the configuration has been changed and not been saved.  
- For `/Username[:password]`, specify the username and password. These must be associated with an account on the FTP server. For more information, see the “Preparing to Download or Upload an Image File By Using FTP” section on page B-27.  
- For `/location`, specify the IP address of the FTP server.  
- For `/directory/image-name.tar`, specify the directory (optional) and the image to download. Directory and image names are case sensitive. |
Working with Software Images

Chapter B  Working with the Cisco IOS File System, Configuration Files, and Software Images

The algorithm installs the downloaded image onto the system board flash device (flash:). The image is placed into a new directory named with the software version string, and the BOOT environment variable is updated to point to the newly installed image.

If you kept the old image during the download process (you specified the /leave-old-sw keyword), you can remove it by entering the delete /force /recursive filesystem:/file-url privileged EXEC command. For filesystem, use flash: for the system board flash device. For file-url, enter the directory name of the old software image. All the files in the directory and the directory are removed.

Caution
For the download and upload algorithms to operate properly, do not rename image names.

Uploading an Image File By Using FTP

You can upload an image from the switch to an FTP server. You can later download this image to the same switch or to another switch of the same type.

Beginning in privileged EXEC mode, follow these steps to upload an image to an FTP server:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Verify that the FTP server is properly configured by referring to the “Preparing to Download or Upload a Configuration File By Using FTP” section on page B-12.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Log into the switch through the console port or a Telnet session.</td>
</tr>
<tr>
<td>Step 3 configure terminal</td>
<td>Enter global configuration mode. This step is required only if you override the default remote username or password (see Steps 4, 5, and 6).</td>
</tr>
<tr>
<td>Step 4 ip ftp username username</td>
<td>(Optional) Change the default remote username.</td>
</tr>
<tr>
<td>Step 5 ip ftp password password</td>
<td>(Optional) Change the default password.</td>
</tr>
<tr>
<td>Step 6 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 7 archive upload-sw ftp:[//username:password@]location]/directory]/image-name.tar</td>
<td>Upload the currently running switch image to the FTP server.</td>
</tr>
</tbody>
</table>

- For //username:password, specify the username and password. These must be associated with an account on the FTP server. For more information, see the “Preparing to Download or Upload an Image File By Using FTP” section on page B-27.

- For @location, specify the IP address of the FTP server.

- For directory]/image-name.tar, specify the directory (optional) and the name of the software image to be uploaded. Directory and image names are case sensitive. The image-name.tar is the name of the software image to be stored on the server.

The archive upload-sw command builds an image file on the server by uploading the info file and the Cisco IOS image file. After these files are uploaded, the upload algorithm creates the tar file format.
For the download and upload algorithms to operate properly, do not rename image names.

Copying Image Files By Using RCP

You can download a switch image from an RCP server or upload the image from the switch to an RCP server.

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

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

Note

Instead of using the `copy` privileged EXEC command or the `archive tar` privileged EXEC command, we recommend using the `archive download-sw` and `archive upload-sw` privileged EXEC commands to download and upload software image files.

This section includes this information:

- Preparing to Download or Upload an Image File By Using RCP, page B-31
- Downloading an Image File By Using RCP, page B-32
- Uploading an Image File By Using RCP, page B-34

Preparing to Download or Upload an Image File By Using RCP

RCP provides another method of downloading and uploading image files between remote hosts and the switch. Unlike TFTP, which uses UDP, a connectionless protocol, RCP uses TCP, which is connection-oriented.

To use RCP to copy files, the server from or to which you will be copying files must support RCP. The RCP copy commands rely on the `rsh` server (or daemon) on the remote system. To copy files by using RCP, you do not need to create a server for file distribution as you do with TFTP. You only need to have access to a server that supports the remote shell (`rsh`). (Most UNIX systems support `rsh`.) Because you are copying a file from one place to another, you must have read permission on the source file and write permission on the destination file. If the destination file does not exist, RCP creates it for you.

RCP requires a client to send a remote username on each RCP request to a server. When you copy an image from the switch to a server by using RCP, the Cisco IOS software sends the first valid username in this list:

- The username specified in the `archive download-sw` or `archive upload-sw` privileged EXEC command if a username is specified.
- The username set by the `ip rcmd remote-username username` global configuration command if the command is entered.
- The remote username associated with the current TTY (terminal) process. For example, if the user is connected to the router through Telnet and was authenticated through the `username` command, the switch software sends the Telnet username as the remote username.
- The switch hostname.
For the RCP copy request to execute successfully, an account must be defined on the network server for
the remote username. If the server has a directory structure, the image file is written to or copied from
the directory associated with the remote username on the server. For example, if the image file resides
in the home directory of a user on the server, specify that user's name as the remote username.

Before you begin downloading or uploading an image file by using RCP, do these tasks:

- Ensure that the workstation acting as the RCP server supports the remote shell (rsh).
- Ensure that the switch has a route to the RCP server. The switch and the server must be in the same
subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the
RCP server by using the ping command.
- If you are accessing the switch through the console or a Telnet session and you do not have a valid
username, make sure that the current RCP username is the one that you want to use for the RCP
download. You can enter the show users privileged EXEC command to view the valid username. If
you do not want to use this username, create a new RCP username by using the ip rcmd
remote-username username global configuration command to be used during all archive
operations. The new username is stored in NVRAM. If you are accessing the switch through a Telnet
session and you have a valid username, this username is used, and there is no need to set the RCP
username. Include the username in the archive download-sw or archive upload-sw privileged
EXEC command if you want to specify a username only for that operation.
- When you upload an image to the RCP to the server, it must be properly configured to accept the
RCP write request from the user on the switch. For UNIX systems, you must add an entry to the
.rhosts file for the remote user on the RCP server. For example, suppose the switch contains these
configuration lines:

```
hostname Switch1
ip rcmd remote-username User0
```

If the switch IP address translates to Switch1.company.com, the .rhosts file for User0 on the RCP
server should contain this line:

```
Switch1.company.com Switch1
```

For more information, see the documentation for your RCP server.

## Downloading an Image File By Using RCP

You can download a new image file and replace or keep the current image.

Beginning in privileged EXEC mode, follow Steps 1 through 6 to download a new image from an RCP
server and overwrite the existing image. To keep the current image, go to Step 6.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Verify that the RCP server is properly configured by referring to the &quot;Preparing to Download or Upload an Image File By Using RCP&quot; section on page B-31.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Log into the switch through the console port or a Telnet session.</td>
</tr>
<tr>
<td>Step 3</td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>This step is required only if you override the default remote username (see Steps 4 and 5).</td>
</tr>
<tr>
<td>Step 4</td>
<td>ip rcmd remote-username username</td>
</tr>
<tr>
<td></td>
<td>(Optional) Specify the remote username.</td>
</tr>
</tbody>
</table>
Step 5  
end  

Step 6  
archive download-sw /overwrite /reload  
rcp:////[/username@]location[/directory]image-name.tar  

Step 7  
archive download-sw /leave-old-sw /reload  
rcp:////[/username@]location[/directory]image-name.tar  

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>archive download-sw /overwrite /reload rcp://[/username@]location[/directory]image-name.tar</td>
<td>Download the image file from the RCP server to the switch, and overwrite the current image.</td>
</tr>
<tr>
<td>archive download-sw /leave-old-sw /reload rcp://[/username@]location[/directory]image-name.tar</td>
<td>Download the image file from the RCP server to the switch, and keep the current image.</td>
</tr>
</tbody>
</table>

- The /overwrite option overwrites the software image in flash memory with the downloaded image.
- The /reload option reloads the system after downloading the image unless the configuration has been changed and not been saved.
- For /username, specify the username. For the RCP copy request to execute successfully, an account must be defined on the network server for the remote username. For more information, see the “Preparing to Download or Upload an Image File By Using RCP” section on page B-31.
- For @location, specify the IP address of the RCP server.
- For /directory[/image-name.tar], specify the directory (optional) and the image to download. Directory and image names are case sensitive.

The download algorithm verifies that the image is appropriate for the switch model and that enough DRAM is present, or it aborts the process and reports an error. If you specify the /overwrite option, the download algorithm removes the existing image on the flash device whether or not it is the same as the new one, downloads the new image, and then reloads the software.

**Note**  
If the flash device has sufficient space to hold two images and you want to overwrite one of these images with the same version, you must specify the /overwrite option.

If you specify the /leave-old-sw, the existing files are not removed. If there is not enough room to install the new image and keep the running image, the download process stops, and an error message appears.
Chapter B  Working with the Cisco IOS File System, Configuration Files, and Software Images

Working with Software Images

The algorithm installs the downloaded image onto the system board flash device (flash:). The image is placed into a new directory named with the software version string, and the BOOT environment variable is updated to point to the newly installed image.

If you kept the old software during the download process (you specified the /leave-old-sw keyword), you can remove it by entering the delete /force /recursive filesystem:file-url privileged EXEC command. For filesystem, use flash: for the system board flash device. For file-url, enter the directory name of the old software image. All the files in the directory and the directory are removed.

Caution

For the download and upload algorithms to operate properly, do not rename image names.

Uploading an Image File By Using RCP

You can upload an image from the switch to an RCP server. You can later download this image to the same switch or to another switch of the same type.

Beginning in privileged EXEC mode, follow these steps to upload an image to an RCP server:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Verify that the RCP server is properly configured by referring to the “Preparing to Download or Upload an Image File By Using RCP” section on page B-31.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Log into the switch through the console port or a Telnet session.</td>
</tr>
<tr>
<td>Step 3</td>
<td>configure terminal Enter global configuration mode. This step is required only if you override the default remote username (see Steps 4 and 5).</td>
</tr>
<tr>
<td>Step 4</td>
<td>ip rcmd remote-username username (Optional) Specify the remote username.</td>
</tr>
<tr>
<td>Step 5</td>
<td>end Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 6</td>
<td>archive upload-sw rcp://[username@]location[/directory]/ imagename.tar Upload the currently running switch image to the RCP server.</td>
</tr>
<tr>
<td></td>
<td>• For [username], specify the username; for the RCP copy request to execute, an account must be defined on the network server for the remote username. For more information, see the “Preparing to Download or Upload an Image File By Using RCP” section on page B-31.</td>
</tr>
<tr>
<td></td>
<td>• For @location, specify the IP address of the RCP server.</td>
</tr>
<tr>
<td></td>
<td>• For [directory]/imagename.tar, specify the directory (optional) and the name of the software image to be uploaded. Directory and image names are case sensitive.</td>
</tr>
<tr>
<td></td>
<td>• The imagename.tar is the name of software image to be stored on the server.</td>
</tr>
</tbody>
</table>

The archive upload-sw privileged EXEC command builds an image file on the server by uploading the info file and the Cisco IOS image file. After these files are uploaded, the upload algorithm creates the tar file format.

Caution

For the download and upload algorithms to operate properly, do not rename image names.
Unsupported Commands in Cisco IOS Release 12.2(55)SE

This appendix lists some of the command-line interface (CLI) commands that are displayed when you enter the question mark (?) at the Catalyst 3750 Metro switch prompt but are not supported in this release, either because they are not tested, or because of Catalyst 3750 Metro switch hardware limitations. This is not a complete list. The unsupported commands are listed by software feature and command mode.

Access Control Lists

Unsupported Privileged EXEC Commands

access-enable [host] [timeout minutes]
access-template [access-list-number | name] [dynamic-name] [source] [destination] [timeout minutes]
clear access-template [access-list-number | name] [dynamic-name] [source] [destination].

Unsupported Global Configuration Commands

access-list rate-limit acl-index {precedence | mask prec-mask}
access-list dynamic extended

ARP

Unsupported Global Configuration Commands

arp ip-address hardware-address smds
arp ip-address hardware-address srp-a
arp ip-address hardware-address srp-b
ip arp track
Unsupported Interface Configuration Commands

arp probe
ip probe proxy

Boot Loader Commands

Unsupported User EXEC Command

verify

Unsupported Global Configuration Command

boot buffersize

CGMP

Unsupported Privileged EXEC Command

clear ip cgmp

Unsupported Interface Configuration Commands

ip cgmp
Clustering

Unsupported Global Configuration Command

- cluster commander-address
- cluster discovery hop-count
- cluster enable
- cluster holdtime
- cluster member
- cluster outside-interface
- cluster run
- cluster standby-group
- cluster timer

Unsupported Privileged EXEC Commands

- show cluster
- show cluster candidates
- show cluster members

Debug

Unsupported Privileged EXEC Commands

- debug cluster
- debug platform cli-redirection main
- debug platform configuration
- debug platform ipc
- debug platform led stack

Embedded Event Manager

Unsupported Privileged EXEC Commands

- `event manager update user policy [policy-filename | group [group name expression]] | repository [url location]`

Parameters are not supported for this command:
event manager run [policy name] <parameter1>... <parameter15>

Unsupported Global Configuration Commands

no event manager directory user repository [url location ]
event manager applet [applet-name] maxrun

Unsupported Commands in Applet Configuration Mode

no event interface name [interface-name] parameter [counter-name] entry-val [entry counter value]
entry-op {gt|ge|eq|ne|lt|le} [entry-type {increment | rate | value} [exit-val [exit value] exit-op
{gt|ge|eq|ne|lt|le} exit-type [increment | rate | value]]average-factor <average-factor-value>]
no trigger
tag

FallBack Bridging

Unsupported Privileged EXEC Commands

clear bridge [bridge-group] multicast [router-ports | groups | counts] [group-address] [interface-unit] [counts]
clear vlan statistics
show bridge [bridge-group] circuit-group [circuit-group] [src-mac-address] [dst-mac-address]
show bridge [bridge-group] multicast [router-ports | groups] [group-address]
show bridge vlan
show interfaces crb
show interfaces {ethernet | fastethernet} [interface | slot/port] irb
show subscriber-policy range

Unsupported Global Configuration Commands

bridge bridge-group acquire
bridge bridge-group address mac-address {forward | discard} [interface-id]
bridge bridge-group aging-time seconds
bridge bridge-group bitswap_l3_addresses
bridge bridge-group bridge ip
bridge bridge-group circuit-group circuit-group pause milliseconds
bridge bridge-group circuit-group circuit-group source-based
bridge cmf
bridge crb
bridge bridge-group domain domain-name
bridge irb
bridge bridge-group mac-address-table limit number
bridge bridge-group multicast-source
bridge bridge-group protocol dec
bridge bridge-group route protocol
bridge bridge-group subscriber policy policy
subscriber-policy policy [[no | default] packet [permit | deny]]

Unsupported Interface Configuration Commands

bridge-group bridge-group cbus-bridging
bridge-group bridge-group circuit-group circuit-number
bridge-group bridge-group input-address-list access-list-number
bridge-group bridge-group input-lat-service-deny group-list
bridge-group bridge-group input-lat-service-permit group-list
bridge-group bridge-group input-lsap-list access-list-number
bridge-group bridge-group input-pattern-list access-list-number
bridge-group bridge-group input-type-list access-list-number
bridge-group bridge-group lat-compression
bridge-group bridge-group output-address-list access-list-number
bridge-group bridge-group output-lat-service-deny group-list
bridge-group bridge-group output-lat-service-permit group-list
bridge-group bridge-group output-lsap-list access-list-number
bridge-group bridge-group output-pattern-list access-list-number
bridge-group bridge-group output-type-list access-list-number
bridge-group bridge-group sse
bridge-group bridge-group subscriber-loop-control
bridge-group bridge-group subscriber-trunk
bridge bridge-group lat-service-filtering
frame-relay map bridge dlei broadcast
interface bvi bridge-group
x25 map bridge x.121-address broadcast [options-keywords]
HSRP

Unsupported Global Configuration Commands

interface Async
interface BVI
interface Dialer
interface Group-Async
interface Lex
interface Multilink
interface Virtual-Template
interface Virtual-Tokenring

Unsupported Interface Configuration Commands

mtu
standby mac-refresh seconds
standby use-bia

IEEE 802.1ad

Unsupported Interface Configuration Commands

ethernet dot1ad isolate

IEEE 802.1x

Unsupported Global Configuration Command

dot1x critical

Unsupported Interface Configuration Commands

dot1x control-direction
dot1x critical
dot1x host-mode multi-domain
Note
Entering this command can put the port in error-disabled state.

```
mab [eap \timeout activity \{value\}] interface configuration command
```

Note
The switch does not support IEEE 802.1x MAC authentication bypass.

```
dot1x pae
dot1x host-mode multi-domain
```

## IGMP Snooping

### Unsupported Global Configuration Commands

- `ip igmp snooping report-suppression`
- `ip igmp snooping source-only-learning`
- `ip igmp snooping tcn`

### Interfaces

### Unsupported Privileged EXEC Command

```
show interfaces [interface-id | vlan vlan-id] [crb | fair-queue | irb | mac-accounting | precedence | irb | random-detect | rate-limit | shape]
```

### Unsupported Global Configuration Command

```
interface tunnel
```

### Unsupported Interface Configuration Commands

```
bandwidth \{bandwidth-kbps | percent percent\}
random-detect [dscp-based | precedence-based]
random-detect dscp dscp min-threshold max-threshold mark-prob-denominator
random-detect exponential-weighting-constant weight
random-detect precedence ip-precedence min-threshold max-threshold mark-prob-denominator
switchport broadcast level
switchport multicast level
```
switchport unicast level

Note
The switchport broadcast, switchport multicast, and switchport unicast commands have been replaced by the storm-control {broadcast | multicast | unicast} level level [.level] interface configuration command.

transmit-interface type number

IP Multicast Routing

Unsupported Privileged EXEC Commands

clear ip rtp header-compression [type number]
The debug ip packet command displays packets received by the switch CPU. It does not display packets that are hardware-switched.
The debug ip mcache command affects packets received by the switch CPU. It does not display packets that are hardware-switched.
The debug ip mpacket [detail] [access-list-number [group-name-or-address]] command affects only packets received by the switch CPU. Because most multicast packets are hardware-switched, use this command only when you know that the route will forward the packet to the CPU.

d debug ip pim atm
show frame-relay ip rtp header-compression [interface type number]
The show ip mcache command displays entries in the cache for those packets that are sent to the switch CPU. Because most multicast packets are switched in hardware without CPU involvement, you can use this command, but multicast packet information is not displayed.
The show ip mpacket commands are supported but are only useful for packets received at the switch CPU. If the route is hardware-switched, the command has no effect because the CPU does not receive the packet and cannot display it.

show ip pim vc [group-address | name] [type number]
show ip rtp header-compression [type number] [detail]

Unsupported Global Configuration Commands

ip pim accept-rp {address | auto-rp} [group-access-list-number]
ip pim message-interval seconds
ip pim register-rate-limit
Unsupported Interface Configuration Commands

frame-relay ip rtp header-compression [active | passive]
frame-relay map ip ip-address dlci [broadcast] compress
frame-relay map ip ip-address dlci rtp header-compression [active | passive]
ip igmp helper-address ip-address
ip multicast helper-map { group-address | broadcast } { broadcast-address | multicast-address }
extended-access-list-number
ip multicast rate-limit { in | out } { video | whiteboard } [ group-list access-list ] [ source-list access-list ] kbps
ip multicast ttl-threshold ttl-value (instead, use the ip multicast boundary access-list-number interface configuration command)
ip multicast use-functional
ip pim minimum-vc-rate pps
ip pim multipoint-signalling
ip pim nbma-mode
ip pim vc-count number
ip rtp compression-connections number
ip rtp header-compression [passive]

IP Unicast Routing

Unsupported Privileged EXEC or User EXEC Commands

clear ip accounting [checkpoint]
clear ip bgp address flap-statistics
clear ip bgp prefix-list
show cef [drop | not-cef-switched]
show ip accounting [checkpoint] [output-packets | access-violations]
show ip bgp dampened-paths
show ip bgp inconsistent-as
show ip bgp regexp regular expression

Unsupported Global Configuration Commands

ip arp track
ip accounting-list ip-address wildcard
ip accounting-transits count
ip cef accounting [per-prefix] [non-recursive]
ip cef traffic-statistics [load-interval seconds] [update-rate seconds]
ip flow-aggregation
ip flow-cache
ip flow-export
ip gratuitous-arps
ip local
ip reflexive-list
ip route dest ip mask next-hop track object-num
router egp
router-isis
router iso-igrp
router mobile
router odr
router static

Unsupported Interface Configuration Commands

dampening
ip accounting
ip accounting precedence {input | output}
ip load-sharing [per-packet]
ip mtu bytes
ip ospf dead-interval minimal hello-multiplier multiplier
ip route-cache
ip verify
ip unnumbered type number
All ip security commands

Unsupported BGP Router Configuration Commands

default-information originate
neighbor advertise-map
neighbor allowas-in
neighbor default-originate
neighbor description
network backdoor
table-map
Unsupported Route Map Commands

match route-type for policy-based routing (PBR)
set automatic-tag
set dampening half-life reuse suppress max-suppress-time
set default interface interface-id [interface-id.....]
set interface interface-id [interface-id.....]
set ip default next-hop ip-address [ip-address.....]
set ip destination ip-address mask
set ip next-hop verify-availability
set ip precedence value
set ip qos-group
set metric-type internal
set origin
set metric-type internal

Miscellaneous

Unsupported User EXEC Commands

verify

Unsupported Privileged EXEC Command

file verify auto

Unsupported User EXEC Command

show mac-address-table multicast

Unsupported Global Configuration Commands

errdisable detect cause dhcp-rate-limit
errdisable recovery cause dhcp-rate-limit
errdisable recovery cause unicast flood
memory reserve critical
MPLS

Unsupported Privileged EXEC or User EXEC Commands

- `debug ip rsvp hello [bfd | detail | stats]`
- `debug ip rsvp sso`
- `debug mpls traffic-eng exp`
- `debug mpls traffic-eng forwarding-adjacency`
- `debug mpls traffic-eng ha`
- `show ip rsvp fast-route`
- `show ip rsvp hello [instance | statistics]`
- `show mpls traffic-eng exp`
- `show mpls traffic-eng forwarding-adjacency`

Unsupported Global Configuration Commands

- `ip rsvp signalling hello [bfd | graceful-restart]`
- `mpls traffic-eng auto-bw`
- `mpls traffic-eng lsp`

Unsupported Interface Configuration Commands

Physical Interfaces

- `ip rsvp bandwidth {mam | rdm}`
- `ip rsvp signalling hello [bfd | dscp | fast-reroute | graceful-restart | refresh | reroute]`
- `mpls traffic-eng srlg`

Tunnel Interfaces

- `tunnel mpls traffic-eng auto-bw`
- `tunnel mpls traffic-eng backup-bw`
- `tunnel mpls traffic-eng exp`
- `tunnel mpls traffic-eng exp-bundle`
- `tunnel mpls traffic-eng forwarding-adjacency`
- `tunnel mpls traffic-eng path-option dynamic attributes`
- `tunnel mpls traffic-eng path-option explicit name attributes`
- `tunnel mpls traffic-eng path-selection`
Unsupported Routing Commands

interface auto-template
mpsl traffic-eng mesh-group (ISIS mode)
mpsl traffic-eng multicast-intact (ISIS mode and OSPF mode)
tunnel destination mesh-group

MSDP

Unsupported Privileged EXEC Commands

show access-expression
show exception
show location
show pm LINE
show smf [interface-id]
show subscriber-policy [policy-number]
show template [template-name]

Unsupported Global Configuration Commands

ip msdp default-peer ip-address | name [prefix-list list] (Because BGP/MBGP is not supported, use the ip msdp peer command instead of this command.)

QoS

Unsupported Policy-Map Configuration Command

class class-default where class-default is the class-map-name.

RADIUS

Unsupported Global Configuration Commands

aaa nas port extended
aaa authentication feature default enable
aaa authentication feature default line
Unsupported Commands in Cisco IOS Release 12.2(55)SE

**SNMP**

Unsupported Global Configuration Commands

- `snmp-server enable informs`
- `snmp-server enable traps flash insertion`
- `snmp-server enable traps flash removal`
- `snmp-server ifindex persist`

**Spanning Tree**

Unsupported Global Configuration Commands

- `spanning-tree etherchannel guard misconfig`
- `spanning-tree pathcost method {long | short}`

Unsupported Interface Configuration Command

- `spanning-tree stack-port`

**Virtual Forwarding Infrastructure (VFI)**

Unsupported Global Configuration Commands

```
l2 vfi vfi-name manual
```
All VFI configuration mode commands

Unsupported Privileged EXEC Commands

- `debug vfi`
- `show vfi`
VLAN

Unsupported vlan-config Command

private-vlan

Unsupported Privileged EXEC Command

show running-config vlan

Unsupported User EXEC Command

show vlan ifindex

VTP

Unsupported Privileged EXEC Command

vtp {password password | pruning | version number} private-vlan

Note

This command has been replaced by the vtp global configuration command.
INDEX

A
abbreviating commands 2-3
ABRs 36-23
access-class command 33-19
access control entries
   See ACEs
access control entry (ACE) 39-3
access-denied response, VMPS 11-28
access groups
   applying ACLs to interfaces 33-20
      IP 33-20
      Layer 2 33-20
      Layer 3 33-20
access lists
   See ACLs
access ports
   and Layer 2 protocol tunneling 15-20
   defined 9-2
accounting
   with IEEE 802.1x 8-5, 8-29
   with RADIUS 7-27
   with TACACS+ 7-11, 7-16
ACEs
   and QoS 34-11
   defined 33-2
   Ethernet 33-2
   IP 33-2
ACLs
   ACEs 33-2
any keyword 33-12
   applying
      on bridged packets 33-38
      on multicast packets 33-40
      on routed packets 33-39
      on switched packets 33-38
      time ranges to 33-16
      to an interface 33-19, 39-7
      to IPv6 interfaces 39-7
      to QoS 34-11
classifying traffic for QoS 34-63
comments in 33-18
compiling 33-22
configuring with VLAN maps 33-37
defined 33-1, 33-7
examples of 33-22, 34-63
extended IP
   configuring for QoS classification 34-65
   creating 33-9
   matching criteria 33-7
host keyword 33-12
IP
   applying to interfaces 33-19
   creating 33-7
   fragments and QoS guidelines 34-53
   implicit deny 33-9, 33-13, 33-15
   implicit masks 33-9
   matching criteria 33-7
   named 33-14
   terminal lines, setting on 33-18
   undefined 33-20
   violations, logging 33-15
IPv6
- applying to interfaces 39-7
- configuring 39-3, 39-4
- displaying 39-8
- interactions with other features 39-4
- limitations 39-3
- matching criteria 39-3
- named 39-3
- precedence of 39-2
- supported 39-2
- unsupported features 39-3
- limiting actions 33-37
- logging messages 33-9
- log keyword 33-15
- MAC extended 33-27, 34-66
  - matching 33-7, 33-20, 39-3
  - monitoring 33-40, 39-8
  - named 33-14
  - named, IPv6 39-3
  - names 39-4
  - number per QoS class map 34-53
  - numbers 33-7
  - port 33-2, 39-1
  - precedence of 33-2
  - QoS 34-11, 34-63
  - resequencing entries 33-14
  - router 33-2, 39-1
- standard IP
  - configuring for QoS classification 34-64
  - creating 33-8
  - matching criteria 33-7
  - supported features 33-21
  - time ranges 33-16
  - unsupported features 33-6
  - unsupported features, IPv6 39-3
  - using router ACLs with VLAN maps 33-36
- VLAN maps
  - configuration guidelines 33-30
  - configuring 33-29

active link 20-4, 20-5, 20-6
active links 20-2
active router 40-1
active traffic monitoring, IP SLAs 41-1
address aliasing 23-2
addresses
  - displaying the MAC address table 5-30
    - dynamic
      - accelerated aging 16-8
      - changing the aging time 5-21
      - default aging 16-8
      - defined 5-19
      - learning 5-20
      - removing 5-22
    - IPv6 37-2
    - MAC, discovering 5-31
    - multicast
      - group address range 45-3
      - STP address management 16-8
    - static
      - adding and removing 5-27
      - defined 5-19
  - address resolution 5-31, 36-7
Address Resolution Protocol
  - See ARP

administrative distances
  - defined 36-110
  - OSPF 36-32
  - routing protocol defaults 36-101
administrative VLAN
  - REP, configuring 19-9
administrative VLAN, REP 19-9
advertisements
  - CDP 25-1
  - LLDP 26-2
  - RIP 36-18
  - VTP 11-19, 12-3
age timer, REP 19-8
aggregatable global unicast addresses  37-3
aggregate addresses, BGP  36-59
aggregated ports
  See EtherChannel
aggregate policers  34-79
aging, accelerating  16-8
aging time
  accelerated
    for MSTP  17-23
    for STP  16-8, 16-21
MAC address table  5-21
maximum
  for MSTP  17-23, 17-24
  for STP  16-21
alarms, RMON  29-3
allowed-VLAN list  11-21
Any Transport over MPLS
  See AToM
area border routers
  See ABRs
area routing
  IS-IS  36-64
  ISO IGRP  36-64
ARP
  configuring  36-8
  defined  5-31, 36-7
  encapsulation  36-9
  static cache configuration  36-8
ARP table
  address resolution  5-31
  managing  5-31
ASBRs  36-23
AS-path filters, BGP  36-54
asymmetrical links, and 802.1Q tunneling  15-4
AToM  44-40
AToM VCCV
  components  44-24
  configuring  44-29
  described  44-24
attributes, RADIUS
  vendor-proprietary  7-29
  vendor-specific  7-28
authentication
  EIGRP  36-40
  HSRP  40-9
  Kerberos  7-31
  local mode with AAA  7-35
  NTP associations  5-4
  RADIUS
    key  7-20
    login  7-22
  TACACS+
    defined  7-11
    key  7-12
    login  7-13
  See also port-based authentication
authentication failed VLAN
  See restricted VLAN
authentication keys, and routing protocols  36-111
authentication manager
  single session ID  8-14
authoritative time source, described  5-2
authorization
  with RADIUS  7-26
  with TACACS+  7-11, 7-15
authorized ports with IEEE 802.1x  8-4
autoconfiguration  3-3
auto enablement  8-13
automatic QoS
  See QoS
autonegotiation
  interface configuration guidelines  9-13
  mismatches  48-7
autonomous system boundary routers
  See ASBRs
autonomous systems, in BGP  36-47
Auto-RP, described  45-6
auxiliary VLAN
See voice VLAN availability features 1-4

B

BackboneFast
  described 18-5
  enabling 18-13
backup interfaces
  See Flex Links
backup links 20-2
backup static routing, configuring 42-11
banners
  configuring
    login 5-19
    message-of-the-day login 5-18
  default configuration 5-17
  when displayed 5-17
Berkeley r-tools replacement 7-46
BGP
  aggregate addresses 36-59
  aggregate routes, configuring 36-59
  CIDR 36-59
  clear commands 36-63
  community filtering 36-56
  configuring neighbors 36-58
  configuring routing sessions 44-9
  default configuration 36-45, 36-75, 36-76
  described 36-44
  enabling 36-47
  monitoring 36-63
  multipath support 36-51
  neighbors, types of 36-47
  path selection 36-51
  peers, configuring 36-58
  prefix filtering 36-55
  resetting sessions 36-50
  route dampening 36-62
  route maps 36-53
  route reflectors 36-61
  routing domain confederation 36-60
  routing session with multi-VRF CE 36-93
  show commands 36-63
  supernets 36-59
  Version 4 36-44
  binding database
    address, DHCP server
      See DHCP, Cisco IOS server database
    DHCP snooping
      See DHCP snooping binding database
  bindings
    address, Cisco IOS DHCP server 21-6
    DHCP snooping database 21-6
    IP source guard 21-16
  binding table, DHCP snooping
    See DHCP snooping binding database
  blocking packets 24-7
  Boolean expressions in tracked lists 42-4
booting
  boot loader, function of 3-2
  boot process 3-1
  manually 3-17
  specific image 3-17
  boot loader
    accessing 3-18
    described 3-2
    environment variables 3-18
    prompt 3-18
    trap-door mechanism 3-2
  bootstrap router (BSR), described 45-7
Border Gateway Protocol
  See BGP
BPDU
  error-disabled state 18-2
  filtering 18-3
  RSTP format 17-11
BPDU filtering
  described 18-3
enabling 18-12
BPDU guard
  described 18-2
  enabling 18-11
bridged packets, ACLs on 33-38
bridge groups
  See fallback bridging
bridge protocol data unit
  See BPDU
broadcast flooding 36-15
broadcast packets
  directed 36-12
  flooded 36-12
broadcast storm-control command 24-4
broadcast storms 24-1, 36-12
bulk statistics
  file 31-6
  object list, configuring 31-19
  object list, described 31-6
  schema, configuring 31-19
  schema, described 31-6
  transfer 31-21
bulk-statistics
  defined 31-6
bulkstat object-list 31-19
bulkstat schema 31-20
bypass mode, Layer 2 protocol-tunneling 15-17, 15-21
described 34-39
CDP
  and trusted boundary 34-60
  configuring 25-2
  default configuration 25-2
  defined with LLDP 26-1
  described 25-1
  disabling for routing device 25-3, 25-4
  enabling and disabling
    on an interface 25-4
    on a switch 25-3
Layer 2 protocol tunneling 15-17
monitoring 25-4
overview 25-1
transmission timer and holdtime, setting 25-2
updates 25-2
CEF
  described 36-98
IPv6 37-18
CFM
  and Ethernet OAM, configuring 43-51
  and Ethernet OAM interaction 43-50
  and OAM manager 43-43
  and other features 43-8
  and tunnels 43-8
  clearing 43-30
  configuration errors 43-6
  configuration guidelines 43-8
  configuring crosscheck 43-12
  configuring fault alarms 43-16
  configuring port MEP 43-14
  configuring static remote MEP 43-13
  configuring the network 43-8
  continuity check messages 43-5
  crosscheck 43-5
  default configuration 43-7
  defined 43-2
  down MEPs 43-4
draft 1 43-4

cables, monitoring for unidirectional links 27-1
CA trustpoint
  configuring 7-43
  defined 7-41
CBWFQ
  configuring
    with DSCP-based WRED 34-119
    with IP precedence-based WRED 34-123
    with tail drop 34-116

CEF
  described 36-98
IPv6 37-18
EtherChannel support  43-8
fault alarms
  configuring  43-16
  defined  43-5
IP SLAs support for  43-6
IP SLAs with endpoint discovers  43-20
loopback messages  43-5
maintenance association  43-3
maintenance domain  43-2
maintenance point  43-3
manually configuring IP SLAs ping or jitter  43-18
measuring network performance  43-6
  continuity check  43-5
  loopback  43-5
  traceroute  43-5
monitoring  43-30, 43-31
on EtherChannel port channels  43-8
port MEP, configuring  43-14
remote MEPs  43-5
SNMP traps  43-5
static RMEP, configuring  43-13
static RMEP check  43-5
traceroute messages  43-5
types of messages  43-5
up MEPs  43-4
version interoperability  43-6
Y.1731, described  43-23
Cisco Data Collection MIB  31-2
Cisco Discovery Protocol
  See CDP
Cisco Express Forwarding
  See CEF
Cisco Group Management Protocol
  See CGMP
Cisco IOS DHCP server
  See DHCP, Cisco IOS DHCP server
Cisco IOS File System  1-4
Cisco IOS IP SLAs  41-1
Cisco Process MIB  31-2
Cisco Secure ACS configuration guide  8-33
CiscoWorks 2000  1-3, 31-5
CISP  8-13
CIST regional root
  See MSTP
CIST root
  See MSTP
civic location  26-3
class-based weighted fair queueing
  See CBWFQ
classless interdomain routing
  See CIDR
classless routing  36-6
class maps for QoS
  configuring
    hierarchical  34-108
    ingress  34-67
described  34-12, 34-33
displaying  34-102, 34-131
class of service
  See CoS
clearing
  Ethernet CFM  43-30
  interfaces  9-23
CLI
  abbreviating commands  2-3
  command modes  2-1
editing features
   enabling and disabling 2-6
   keystroke editing 2-6
   wrapped lines 2-8
error messages 2-4
filtering command output 2-8
getting help 2-3
history
   changing the buffer size 2-5
   described 2-4
   disabling 2-5
   recalling commands 2-5
no and default forms of commands 2-4

Client Information Signalling Protocol
   See CISP
client mode, VTP 12-3
client processes, tracking 42-1

CLNS
   See ISO CLNS
clock
   See system clock

CNS
   Configuration Engine
      configID, deviceID, hostname 4-3
      configuration service 4-2
      described 4-1
      event service 4-3
embedded agents
   described 4-5
   enabling automated configuration 4-6
   enabling configuration agent 4-9
   enabling event agent 4-7
for upgrading 4-14

command-line interface
   See CLI
command modes 2-1
commands
   abbreviating 2-3
   no and default 2-4

setting privilege levels 7-8

common session ID
   see single session ID 8-14

community list, BGP 36-14
community ports 13-2
community strings
   configuring 31-8
   overview 31-4
community VLANs 13-2, 13-3
config.text 3-16

configuration examples
   ACLs and VLAN maps 33-32
   IP ACLs 33-22
   multi-VRF-CE 36-94
   network 1-14
   SNMP 31-23
   VLAN maps 33-34
   VMPS 11-29

configuration files
   archiving B-18
   clearing the startup configuration B-18
   creating using a text editor B-9
   default name 3-16
   deleting a stored configuration B-18
   described B-7
downloading
   automatically 3-16
   preparing B-10, B-12, B-15
   reasons for B-8
   using FTP B-12
   using RCP B-16
   using TFTP B-10
guidelines for creating and using B-8
guidelines for replacing and rolling back B-19
invalid combinations when copying B-5
limiting TFTP server access 31-18, 31-19, 31-21, 31-22
obtaining with DHCP 3-8
password recovery disable considerations 7-5
replacing a running configuration B-18, B-19
rolling back a running configuration  B-18, B-19  
specifying the filename  3-16  
system contact and location information  31-17  
types and location  B-9  
uploading  
  preparing  B-10, B-12, B-15  
  reasons for  B-8  
  using FTP  B-13  
  using RCP  B-17  
  using TFTP  B-11  
configuration guidelines  
  applying ACLs  33-19  
  applying MAC ACLs  33-28  
  auto-QoS  34-45  
Auto-RP and BSR  45-11  
CFM  43-8  
EtherChannel  35-9  
Ethernet OAM  43-34  
fallback bridging  47-3  
hierarchical QoS  34-103  
HSRP  
  authentication and timers  40-9  
  interfaces  40-4  
  priority  40-6  
IEEE 802.1Q trunks  11-18  
interface speed and duplex mode  9-13  
IP multicast routing  45-10  
MPLS OAM  44-25  
MPLS TE and fast reroute  44-15  
MPLS VPN  44-7  
MSTP  17-14, 18-10  
multi-VRF CE  36-86  
named ACLs  33-14  
OAM manager  43-44  
port-based authentication  8-16  
port security  24-11  
protected ports  24-6  
pseudowire redundancy  44-47  
REP  19-7  
router ACLs and VLAN maps  33-37  
RSPAN  28-16  
SDM templates  6-4  
SNMP  31-7  
SPAN  28-10  
standard QoS  34-53  
STP  16-12, 18-10  
UDLD  27-4  
VLAN maps  33-30  
VLANs  
  extended-range  11-11  
  normal-range  11-6  
VMPS  11-29  
voice VLAN  14-3  
VTP  12-7  
configuration replacement  B-18  
configuration rollback  B-18  
configuration settings, saving  3-15  
configure terminal command  9-7  
configuring multicast VRFs  36-92  
configuring port-based authentication violation modes  8-18 to 8-19  
configuring small-frame arrival rate  24-5  
congestion-avoidance mechanisms  
  WRED  34-38, 34-119, 34-123  
  WTD  34-19, 34-87, 34-91  
congestion management for QoS  34-38  
connectionless service, and VPNs  44-4  
connections, secure remote  7-36  
Connectivity Fault Management  
  See CFM  
connectivity problems  48-8, 48-9, 48-11  
consistency checks in VTP version 2  12-4  
console port, connecting to  2-9  
control protocol, IP SLAs  41-4  
convergence  
  REP  19-4  
corrupted software, recovery steps with XMODEM  48-2  
CoS
configuring the default port value 34-59
in Layer 2 frames 34-2
override priority 14-5
trust priority 14-5
CoS input queue threshold map for QoS 34-21
CoS output queue threshold map for QoS 34-25
CoS-to-DSCP map for QoS 34-81
counters, clearing interface 9-23
CPU threshold notification 31-23
CPU threshold table 31-2, 31-22
CPU utilization, troubleshooting 48-17
CPU utilization statistics 31-22
crashinfo file 48-17
crosscheck, CFM 43-5, 43-12
cryptographic software image
Kerberos 7-31
SSH 7-36
SSL 7-40
customer edge devices
and Multi-VFR CE 36-84
customer-edge devices
and VPNs 44-3, 44-6
MPLS 44-5

data collection, bulk statistics 31-21
daylight saving time 5-13
debugging
enabling all system diagnostics 48-14
enabling for a specific feature 48-13
redirecting error message output 48-14
using commands 48-13
default commands 2-4
default configuration
auto-QoS 34-41
banners 5-17
BGP 36-45, 36-75, 36-76
booting 3-15

CDP 25-2
CFM 43-7
DHCP 21-8
DHCP option 82 21-8
DHCP snooping 21-8
DHCP snooping binding database 21-8
DNS 5-16
dynamic ARP inspection 22-5
EIGRP 36-37
E-LMI and OAM 43-44
EoMPLS 44-43
EtherChannel 35-9
Ethernet OAM 43-34
fallback bridging 47-3
Flex Links 20-8
hierarchical QoS 34-103
HSRP 40-4
IEEE 802.1Q tunneling 15-4
IEEE 802.1x 8-15
IGMP 45-38
IGMP filtering 23-22
IGMP snooping 23-6, 38-5, 38-6
IGMP throttling 23-22
initial switch information 3-3
IP addressing, IP routing 36-4
IP multicast routing 45-10
IP SLAs 41-6
IP source guard 21-17
IPv6 37-9
IS-IS 36-65
Layer 2 interfaces 9-11
Layer 2 protocol tunneling 15-20
LLDP 26-3
MAC address table 5-21
MAC address-table move update 20-8
MPLS 44-7
MPLS OAM 44-25
MPLS QoS 44-53
MPLS TE and fast reroute 44-15
MSDP 46-4
MSTP 17-14
multi-VRF CE 36-86
MVR 23-16
NTP 5-4
optional spanning-tree features 18-9
OSPF 36-25
password and privilege level 7-2
private VLANs 13-6
RADIUS 7-19
REP 19-7
RIP 36-18
RMON 29-3
RSPAN 28-9
SNMP 31-7
SPAN 28-9
SSL 7-43
standard QoS 34-50
STP 16-11
system message logging 30-3
system name and prompt 5-15
TACACS+ 7-12
UDLD 27-4
VLAN, Layer 2 Ethernet interfaces 11-18
VLAN mapping 15-8
VLANs 11-7
VMPS 11-29
voice VLAN 14-3
VTP 12-6
Y.1731 43-25
default gateway 3-14, 36-10
default networks 36-101
default router preference
See DRP
default routes 36-101
deleting VLANs 11-9
denial-of-service attack 24-1
description command 9-17
designing your network, examples 1-14
destination addresses
in IPv6 ACLs 39-5
destination addresses, in ACLs 33-11
destination-IP address based forwarding, EtherChannel 35-7
destination-MAC address forwarding, EtherChannel 35-7
detecting indirect link failures, STP 18-5
device discovery protocol 25-1, 26-1
DHCP
Cisco IOS server database
configuring 21-14
default configuration 21-8
described 21-6
DHCP for IPv6
See DHCPv6
enabling
relay agent 21-10
server 21-10
DHCP-based autoconfiguration
client request message exchange 3-4
configuring
client side 3-3
DNS 3-7
relay device 3-8
server side 3-6
server-side 21-10
TFTP server 3-7
example 3-9
lease options
for IP address information 3-6
for receiving the configuration file 3-6
overview 3-3
relationship to BOOTP 3-3
DHCP-based autoconfiguration and image update
configuring 3-11 to 3-14
understanding 3-5 to 3-6
DHCP binding database
See DHCP snooping binding database
DHCP binding table
See DHCP snooping binding database
DHCP object tracking, configuring primary interface 42-10
DHCP option 82
  circuit ID suboption 21-5
  configuration guidelines 21-9
  default configuration 21-8
  displaying 21-15
  forwarding address, specifying 21-10
  helper address 21-10
  overview 21-3
  packet format, suboption
    circuit ID 21-5
    remote ID 21-5
  remote ID suboption 21-5
  support for 1-3
DHCP server port-based address allocation
  configuration guidelines 21-26
  default configuration 21-26
  described 21-25
  displaying 21-29
  enabling 21-26
  reserved addresses 21-27
DHCP snooping
  accepting untrusted packets from edge switch 21-3, 21-12
  and private VLANs 21-13
  binding database
    See DHCP snooping binding database
  configuration guidelines 21-9
  default configuration 21-8
  displaying binding tables 21-15
  message exchange process 21-4
  option 82 data insertion 21-3
  trusted interface 21-2
  untrusted interface 21-2
  untrusted messages 21-2
DHCP snooping binding database
  adding bindings 21-14
  binding file
    format 21-7
    location 21-6
  bindings 21-6
  clearing agent statistics 21-15
  configuration guidelines 21-9
  configuring 21-14
  default configuration 21-8
  deleting
    binding file 21-14
    bindings 21-15
    database agent 21-14
  described 21-6
  displaying 21-15
  status and statistics 21-15
  enabling 21-14
  entry 21-6
  renewing database 21-15
  resetting
    delay value 21-14
    timeout value 21-14
DHCP snooping binding table
  See DHCP snooping binding database
DHCPv6
  configuration guidelines 37-14
  default configuration 37-14
  described 37-6
  enabling client function 37-17
  enabling DHCPv6 server function 37-15
Differentiated Services architecture, QoS 34-2
Differentiated Services Code Point
  See DSCP
Diffusing Update Algorithm (DUAL) 36-35
Digital Optical Monitoring
  see DoM
directories
  changing B-3
  creating and removing B-4
  displaying the working B-3
discovery, Ethernet OAM  43-33
Distance Vector Multicast Routing Protocol
  See DVMRP
distribute-list command  38-110
DNS
  and DHCP-based autoconfiguration  3-7
default configuration  5-16
displaying the configuration  5-17
  in IPv6  37-3
overview  5-15
setting up  5-16
DNS-based SSM mapping  45-19, 45-21
DoM
  displaying supported transceivers  9-22
domain names
  DNS  5-15
  VTP  12-7
Domain Name System
  See DNS
domains, ISO IGRP routing  36-64
dot1q-tunnel switchport mode  11-16
double-tagged packets
  802.1Q tunneling  15-2
  Layer 2 protocol tunneling  15-19
downloadable ACL  8-33
downloading
  configuration files
    preparing  B-10, B-12, B-15
    reasons for  B-8
    using FTP  B-12
    using RCP  B-16
    using TFTP  B-10
image files
  deleting old image  B-26
  preparing  B-24, B-27, B-31
  reasons for  B-22
  using FTP  B-28
  using HTTP  B-22
  using RCP  B-32
  using TFTP  B-25
drop threshold for Layer 2 protocol packets  15-20
DRP
  configuring  37-12
  described  37-4
IPv6  37-4
DSCP  34-3
DSCP input queue threshold map for QoS  34-21
DSCP output queue threshold map for QoS  34-25
DSCP-to-CoS map for QoS  34-84
DSCP-to-DSCP-mutation map for QoS  34-85
DSCP transparency  34-61
DTP  11-15
DUAL finite state machine, EIGRP  36-36
dual IPv4 and IPv6 templates  6-2, 37-5
dual-level policy maps
  configuring  34-73
  described  34-15
dual protocol stacks
  IPv4 and IPv6  37-5
  SDM templates supporting  37-6
duplex mode, configuring  9-13
DVMRP
  autosummarization
    configuring a summary address  45-58
    disabling  45-60
  connecting PIM domain to DVMRP router  45-50
  enabling unicast routing  45-54
  interoperability
    with Cisco devices  45-48
    with IOS software  45-8
  mrinfo requests, responding to  45-53
  neighbors
    advertising the default route to  45-52
    discovery with Probe messages  45-48
    displaying information  45-53
    prevent peering with nonpruning  45-56
    rejecting nonpruning  45-54
  overview  45-8
routes
   adding a metric offset  45-60
   advertising all  45-60
   advertising the default route to neighbors  45-52
   caching DVMRP routes learned in report messages  45-54
   changing the threshold for syslog messages  45-57
   deleting  45-61
   displaying  45-62
   favoring one over another  45-60
   limiting the number injected into MBONE  45-57
   limiting unicast route advertisements  45-48
routi ng table  45-9
source distribution tree, building  45-9

tunnels
   configuring  45-50
   displaying neighbor information  45-53
dynamic access ports
   characteristics  11-3
   configuring  11-30
   defined  9-3
dynamic addresses
   See addresses
dynamic ARP inspection
   ARP cache poisoning  22-1
   ARP requests, described  22-1
   ARP spoofing attack  22-1
clearing
   log buffer  22-15
   statistics  22-15
configuration guidelines  22-6
configuring
   ACLs for non-DHCP environments  22-8
   in DHCP environments  22-7
   log buffer  22-12
   rate limit for incoming ARP packets  22-4, 22-10
default configuration  22-5
denial-of-service attacks, preventing  22-10
described  22-1

dynamic routing
   ISO CLNS  36-64
   protocols  36-2
   DHCP snooping binding database  22-2
displaying
   ARP ACLs  22-14
   configuration and operating state  22-14
   log buffer  22-15
   statistics  22-15
   trust state and rate limit  22-14
error-disabled state for exceeding rate limit  22-4
function of  22-2
interface trust states  22-3
log buffer
   clearing  22-15
   configuring  22-12
   displaying  22-15
logging of dropped packets, described  22-4
man-in-the middle attack, described  22-2
network security issues and interface trust states  22-3
priority of ARP ACLs and DHCP snooping entries  22-4
rate limiting of ARP packets
   configuring  22-10
   described  22-4
   error-disabled state  22-4
statistics
   clearing  22-15
   displaying  22-15
validation checks, performing  22-11
dynamic auto trunking mode  11-16
dynamic desirable trunking mode  11-16
Dynamic Host Configuration Protocol
   See DHCP-based autoconfiguration
dynamic port VLAN membership
   described  11-28
   reconfirming  11-31
   troubleshooting  11-33
   types of connections  11-30
dynamic routing
   ISO CLNS  36-64
   protocols  36-2
Dynamic Trunking Protocol
   See DTP

E

EBGP  36-43, 44-6
ECMP tree trace  44-24
ECMP tree trace, configuring  44-37
editing features
   enabling and disabling  2-6
   keystrokes used  2-6
   wrapped lines  2-8
EEM 3.2  32-5
EIGRP
   and IGRP  36-38
   authentication  36-40
   components  36-36
   configuring  36-38
   default configuration  36-37
   definition  36-35
   interface parameters, configuring  36-39
   monitoring  36-42
   stub routing  36-41
ELIN location  26-3
E-LMI
   and OAM Manager  43-43
   CE device configuration  43-49
   configuration guidelines  43-44
   configuring a CE device  43-47
   configuring a PE device  43-47
   default configuration  43-44
   defined  43-42
   enabling  43-47
   information  43-43
   monitoring  43-49
   PE device configuration  43-48
embedded event manager
   3.2  32-5
   actions  32-4
   configuring  32-1, 32-6
   displaying information  32-7
   environmental variables  32-5
   event detectors  32-3
   policies  32-4
   registering and defining an applet  32-6
   registering and defining a TCL script  32-7
   understanding  32-1
   enable password  7-3
   enable secret password  7-3
   encapsulation, in pseudowire redundancy  44-48
   encryption, CipherSuite  7-42
   encryption for passwords  7-3
Enhanced IGRP
   See EIGRP
   enhanced object tracking
   backup static routing  42-11
   commands  42-1
   defined  42-1
   DHCP primary interface  42-10
   HSRP  42-7
   IP routing state  42-2
   IP SLAs  42-9
   line-protocol state  42-2
   network monitoring with IP SLAs  42-11
   routing policy, configuring  42-11
   static route primary interface  42-10
   tracked lists  42-3
   enhanced object tracking static routing  42-10
   enhanced-services interfaces
   See ES interfaces
   environmental variables, embedded event manager  32-5
   environment variables, function of  3-19
EoMPLS
   and 802.1Q tunneling  44-41
   and Layer 2 protocol tunneling  44-42
   and QoS  44-42
   configuring  44-44
   default configuration  44-43
limitations 44-42
monitoring 44-55
packet flow 44-45
QoS 44-51
equal cost multipath tree trace
See ECMP tree trace
equal-cost routing 36-99
error messages during command entry 2-4
ES interfaces 9-3, 9-7, 44-1
EtherChannel
802.3ad, described 35-5
automatic creation of 35-4, 35-5
channel groups
binding physical and logical interfaces 35-3
numbering of 35-3
configuration guidelines 35-9
configuring
Layer 3 physical interfaces 35-14
Layer 3 port-channel logical interfaces 35-13
configuring Layer 2 interfaces 35-10
default configuration 35-9
described 35-2
displaying status 35-20
forwarding methods 35-6, 35-16
interaction
with STP 35-9
with VLANs 35-10
LACP
described 35-4
displaying status 35-20
hot-standby ports 35-18
interaction with other features 35-6
modes 35-5
port priority 35-19
system priority 35-19
Layer 3 interface 36-3
load balancing 35-6, 35-16
logical interfaces, described 35-3
number of interfaces per 35-2
PAgP
aggregate-port learners 35-17
compatibility with Catalyst 1900 35-17
described 35-4
displaying status 35-20
interaction with other features 35-5
learn method and priority configuration 35-17
modes 35-4
silent mode 35-5
port-channel interfaces
described 35-3
numbering of 35-3
port groups 9-5
EtherChannel guard
described 18-7
disabling 18-14
enabling 18-14
Ethernet infrastructure 43-1
Ethernet Link Management Interface
See E-LMI
Ethernet Locked Signal (ETH-LCK) 43-25
Ethernet OAM 43-33
and CFM interaction 43-50
configuration guidelines 43-34
configuring with CFM 43-51
default configuration 43-34
discovery 43-33
enabling 43-34, 43-52
link monitoring 43-33, 43-36
manager 43-1
messages 43-33
protocol
defined 43-32
monitoring 43-42
remote failure indications 43-33, 43-39
remote loopback 43-33, 43-35
templates 43-39
Ethernet OAM protocol 43-1
Ethernet OAM protocol CFM notifications 43-50
Catalyst 3750 Metro Switch Software Configuration Guide

Index

Ethernet operation, administration, and maintenance
   See Ethernet OAM
Ethernet over MPLS
   See EoMPLS
Ethernet Remote Defect Indication (ETH-RDI)  43-24
Ethernet virtual connections
   See EVCs
Ethernet VLANs
   creating  11-8
   defaults and ranges  11-8
   modifying  11-8
EUI  37-3
EVCs
   configuring  43-45
   in CFM domains  43-42
event detectors, embedded event manager  32-3
events, RMON  29-3
examples
   network configuration  1-14
experimental bits, setting MPLS priority with  44-53
extended-range VLANs
   configuration guidelines  11-11
   configuring  11-11
   creating  11-11, 11-12
   defined  11-1
extended system ID
   MSTP  17-17
   STP  16-4, 16-14
extended universal identifier
   See EUI
Extensible Authentication Protocol over LAN  8-1
external BGP
   See EBGP
external neighbors, BGP  36-47
bridge groups
   creating  47-3
   described  47-1
   displaying  47-10
   function of  47-2
   number supported  47-4
   removing  47-4
bridge table
   clearing  47-10
   displaying  47-10
configuration guidelines  47-3
connecting interfaces with  9-7
default configuration  47-3
described  47-1
frame forwarding
   flooding packets  47-2
   forwarding packets  47-2
overview  47-1
protocol, unsupported  47-3
STP
   disabling on an interface  47-9
   forward-delay interval  47-8
   hello BPDU interval  47-8
   interface priority  47-6
   keepalive messages  16-2
   maximum-idle interval  47-9
   path cost  47-7
   VLAN-bridge spanning-tree priority  47-5
   VLAN-bridge STP  47-2
   SVIs and routed ports  47-1
   unsupported protocols  47-3
   VLAN-bridge STP  16-10, 47-1
Fast Convergence  20-3
features
   availability  1-4
   Layer 2 VPN services  1-6
   Layer 3  1-10
   Layer 3 VPN services  1-7
   manageability  1-3

F

fallback bridging
   and protected ports  47-3
Index

management options 1-3
monitoring 1-11
performance 1-2
QoS 1-8
security 1-7
VLAN 1-6
FEC 44-2
FIB 36-98
fiber-optic, detecting unidirectional links 27-1
files
  copying B-4
  crashinfo
description 48-17
displaying the contents of 48-17
  location 48-17
deleting B-5
displaying the contents of B-7
tar
  creating B-5
displaying the contents of B-6
  extracting B-7
  image file format B-23
file system
  displaying available file systems B-2
displaying file information B-3
local file system names B-1
network file system names B-4
setting the default B-3
filtering
  in a VLAN 33-29
IPv6 traffic 39-3, 39-7
non-IP traffic 33-27
  show and more command output 2-8
filters, IP
  See ACLs, IP
flash device, number of B-1
Flex Link Multicast Fast Convergence 20-3
Flex Links
  configuration guidelines 20-8
configuring 20-9
configuring preferred VLAN 20-12
configuring VLAN load balancing 20-11
default configuration 20-8
description 20-1
link load balancing 20-2
monitoring 20-14
VLANs 20-2
flooded traffic, blocking 24-8
flowcharts
  QoS egress queue-set queueing and scheduling 34-23
  QoS hierarchical queues queueing and scheduling 34-37
  QoS hierarchical two-rate policing and marking 34-35
  QoS ingress, single-rate policing and marking 34-15
  QoS ingress classification 34-11
  QoS ingress queueing and scheduling 34-20
flow control 9-14
forward-delay time
  MSTP 17-23
  STP 16-21
forwarding-equivalence class
  See FEC
forwarding equivalence classes 44-3
Forwarding Information Base
  See FIB
forwarding non-routable protocols 47-1
FTP
  accessing MIB files A-4
configuration files
  downloading B-12
  overview B-11
  preparing the server B-12
  uploading B-13
image files
  deleting old image B-30
downloading B-28
  preparing the server B-27
uploading B-30

G

general query 20-5
Generating IGMP Reports 20-3
get-bulk-request operation 31-4
get-next-request operation 31-4, 31-5
get-request operation 31-4, 31-5
get-response operation 31-4

guest VLAN and IEEE 802.1x 8-9

H

hardware limitations and Layer 3 interfaces 9-18
hello time
  MSTP 17-22
  STP 16-20
help, for the command line 2-3
Hierarchical policies 34-40
hierarchical policy maps on SVIs 34-13
  configuring 34-73
  described 34-15

Hierarchical QoS
  See QoS
Hierarchical QoS, and EtherChannels 34-103

history
  changing the buffer size 2-5
  described 2-4
  disabling 2-5
  recalling commands 2-5
history table, level and number of syslog messages 30-9
host ports
  configuring 13-11
  kinds of 13-2
hosts, limit on dynamic ports 11-33
Hot Standby Router Protocol

See HSRP
HP OpenView 1-3
HSRP
  authentication string 40-9
  configuring 40-4
  default configuration 40-4
  definition 40-1
  enabling 40-5
  guidelines 40-4
  monitoring 40-10
  object tracking 42-7
  overview 40-1
  priority 40-6
  routing redundancy 1-10
  support for ICMP redirect messages 40-10
  timers 40-9
  tracking 40-7
HTTP over SSL
  see HTTPS
HTTPS 7-40
  configuring 7-44
  self-signed certificate 7-41
HTTP secure server 7-40

IBGP 36-43, 44-6
ICMP
  IPv6 37-4
  redirect messages 36-10
  time exceeded messages 48-11
  traceroute and 48-11
  unreachable messages 33-19
  unreachable messages and IPv6 39-4
  unreachables and ACLs 33-21
ICMP Echo operation
  configuring 41-11
  IP SLAs 41-11
ICMP ping
executing 48-8
overview 48-8
ICMP Router Discovery Protocol
See IRDP
ICMPv6 37-4
IDS appliances
and ingress RSPAN 28-20
and ingress SPAN 28-13
IEEE 802.1ag 43-2
IEEE 802.1D
See STP
IEEE 802.1p 14-1
IEEE 802.1Q
and trunk ports 9-3
configuration limitations 11-18
encapsulation 11-15
native VLAN for untagged traffic 11-23
tunneling
 compatibility with other features 15-6
defaults 15-4
described 15-2
tunnel ports with other features 15-6
IEEE 802.1s
See MSTP
IEEE 802.1w
See RSTP
IEEE 802.1x
See port-based authentication
IEEE 802.1x accounting 8-29
IEEE 802.3ad
See EtherChannel
IEEE 802.3ah Ethernet OAM discovery 43-1
IEEE 802.3x flow control 9-14
ifIndex values, SNMP 31-6
IGMP
configuring the switch
 as a member of a group 45-38
statically connected member 45-43
controlling access to groups 45-39
default configuration 45-38
deleting cache entries 45-62
displaying groups 45-62
fast switching 45-43
host-query interval, modifying 45-41
joining multicast group 23-3
join messages 23-3
leave processing, enabling 23-10, 38-8
leaving multicast group 23-4
multicast reachability 45-38
overview 45-2
queries 23-3
report suppression
 described 23-5
disabling 23-12, 38-11
Version 1
 changing to Version 2 45-40
described 45-3
Version 2
 changing to Version 1 45-40
described 45-3
maximum query response time value 45-42
pruning groups 45-42
query timeout value 45-42
IGMP filtering
 configuring 23-22
default configuration 23-22
described 23-21
monitoring 23-26
IGMP groups
 configuring filtering 23-25
setting the maximum number 23-24
IGMP helper 1-2, 45-6
IGMP profile
 applying 23-23
configuration mode 23-22
configuring 23-23
IGMP snooping
 and address aliasing 23-2
configuring 23-5
default configuration 23-6, 38-5, 38-6
definition 23-1
enabling and disabling 23-6, 38-6
global configuration 23-6
Immediate Leave 23-5
method 23-7
monitoring 23-12, 38-11
querier
configuration guidelines 23-10
configuring 23-10
VLAN configuration 23-7
IGMP throttling
configuring 23-25
default configuration 23-22
described 23-22
displaying action 23-26
IGP 36-23
IGRP, split horizon 36-22
Immediate Leave, IGMP 23-5
enabling 38-8
initial configuration
defaults 1-12
interface
number 9-7
range macros 9-10
interface command 9-7
interface configuration
REP 19-10
interface configuration mode 2-2
interfaces
configuration guidelines 9-13
configuring 9-7
configuring duplex mode 9-13
configuring speed 9-13
counters, clearing 9-23
described 9-17
descriptive name, adding 9-17
displaying information about 9-22
flow control 9-14
management 1-3
naming 9-17
physical, identifying 9-7
range of 9-8
restarting 9-23
shutting down 9-23
supported 9-7
types of 9-1
interfaces range macro command 9-10
interface types 9-7
Interior Gateway Protocol
See IGP
internal BGP
See IBGP
internal neighbors, BGP 36-47
Internet Control Message Protocol
See ICMP
Internet Group Management Protocol
See IGMP
Internet Protocol version 6
See IPv6
Inter-Switch Link
See ISL
inter-VLAN routing 36-2
Intrusion Detection System
See IDS appliances
inventory management TLV 26-6
ip access group command 33-20
IP ACLs
extended, creating 33-9
for QoS classification 34-11
implicit deny 33-9, 33-13, 33-15
implicit masks 33-9
logging 33-15
named 33-14
standard, creating 33-8
undefined 33-20
virtual terminal lines, setting on 33-18
IP addresses
128-bit 37-2
classes of 36-4
default configuration 36-4
discovering 5-31
for IP routing 36-3
IPv6 37-2
MAC address association 36-7
monitoring 36-16
IP broadcast address 36-14
IP directed broadcasts 36-12
ip igmp profile command 23-22
IP information
assigned
  manually 3-14
  through DHCP-based autoconfiguration 3-3
default configuration 3-3
IP multicast routing
addresses
  all-hosts 45-3
  all-multicast-routers 45-3
  host group address range 45-3
administratively-scoped boundaries, described 45-46
and IGMP snooping 23-1
Auto-RP
  adding to an existing sparse-mode cloud 45-25
  benefits of 45-25
  clearing the cache 45-62
  configuration guidelines 45-11
  filtering incoming RP announcement messages 45-28
  overview 45-6
  preventing candidate RP spoofing 45-28
  preventing join messages to false RPs 45-27
  setting up in a new internetwork 45-25
  using with BSR 45-33
bootstrap router
  configuration guidelines 45-11
  configuring candidate BSRs 45-31
  configuring candidate RPs 45-32
defining the IP multicast boundary 45-30
defining the PIM domain border 45-29
overview 45-7
using with Auto-RP 45-33
Cisco implementation 45-1
  configuring
    basic multicast routing 45-11
    IP multicast boundary 45-46
default configuration 45-10
  enabling
    multicast forwarding 45-12
    PIM mode 45-12
group-to-RP mappings
  Auto-RP 45-6
  BSR 45-7
MBONE
deleting sdr cache entries 45-62
described 45-45
displaying sdr cache 45-63
enabling sdr listener support 45-45
limiting DVMRP routes advertised 45-57
limiting sdr cache entry lifetime 45-45
SAP packets for conference session announcement 45-45
Session Directory (sdr) tool, described 45-45
monitoring
  packet rate loss 45-63
  peering devices 45-63
  tracing a path 45-63
multicast forwarding, described 45-7
PIMv1 and PIMv2 interoperability 45-10
protocol interaction 45-2
reverse path check (RPF) 45-7
routing table
deleting 45-62
displaying 45-62
RP
assigning manually 45-23
configuring Auto-RP 45-25
configuring PIMv2 BSR 45-29
monitoring mapping information 45-34
using Auto-RP and BSR 45-33
statistics, displaying system and network 45-62
See also CGMP
See also DVMRP
See also IGMP
See also PIM

IP phones
and QoS 14-1
automatic classification and queueing 34-41
configuring 14-4
ensuring port security with QoS 34-60
trusted boundary for QoS 34-60

IP Port Security for Static Hosts
on a Layer 2 access port 21-19
on a PVLAN host port 21-23

IP precedence 34-3
IP-precedence-to-DSCP map for QoS 34-82
IP protocols in ACLs 33-11
IP routes, monitoring 36-112

IP routing
connecting interfaces with 9-6
enabling 36-17
IP Service Level Agreements
See IP SLAs
IP Service Level Agreements
See IP SLAs 44-22
IP service levels, analyzing 41-1

IP SLAs
benefits 41-2
CFM endpoint discovery 43-20
configuration guidelines 41-6
configuring manually 44-30
configuring object tracking 42-9
Control Protocol 41-4
default configuration 41-6
definition 44-1
definition 41-1

ECMP tree trace, configuring 44-37
Health Monitor 44-24
ICMP echo operation 41-11
LSP Health Monitor
configuring 44-31
described 44-25
LSP Health Monitor, configuring 44-31
manually configuring CFM ping or jitter 43-18
manually configuring LSP ping 44-34
manually configuring LSP traceroute 44-34
measuring network performance 41-3
monitoring 41-13
monitoring MPLS LSP 44-30
MPLS 44-22
MPLS LSP 44-24
MPLS parameters, configuring 44-31
multioperations scheduling 41-5
object tracking 42-9
operation 41-3
reachability tracking 42-9
responder
  described 41-4
  enabling 41-7
  response time 41-4
  scheduling 41-5
SNMP support 41-2
supported metrics 41-2
threshold monitoring 41-6
track object monitoring agent, configuring 42-11
track state 42-9
UDP jitter operation 41-8

IP source guard
and DHCP snooping 21-15
and EtherChannels 21-18
and IEEE 802.1x 21-18
and port security 21-18
and private VLANs 21-18
and routed ports 21-17
and TCAM entries 21-18
default addressing configuration 36-4
gateways 36-10
networks 36-101
routes 36-101
directed broadcasts 36-12
dynamic routing 36-2
enabling 36-17
EtherChannel Layer 3 interface 36-3
IGP 36-23
inter-VLAN 36-2
IP addressing classes 36-4
configuring 36-3
IPv6 37-3
IRDP 36-11
Layer 3 interfaces 36-3
MAC address and IP address 36-7
passive interfaces 36-109
proxy ARP 36-7
redistribution 36-102
reverse address resolution 36-7
routed ports 36-3
static routing 36-2
steps to configure 36-3
subnet mask 36-5
subnet zero 36-5
supernet 36-5
UDP 36-14
with SVIs 36-3
See also BGP
See also EIGRP
See also IS-IS
See also OSPF
See also RIP
IPv4 and IPv6 dual protocol stacks 37-5
IPv6
ACLs

and trunk interfaces 21-18
and VRF 21-18
binding configuration
   automatic 21-16
   manual 21-16
binding table 21-16
configuration guidelines 21-17
default configuration 21-17
described 21-15
disabling 21-19
displaying bindings 21-25
   configuration 21-25
enabling 21-18, 21-19
filtering
   source IP address 21-16
   source IP and MAC address 21-16
source IP address filtering 21-16
source IP and MAC address filtering 21-16
static bindings
   adding 21-18, 21-19
   deleting 21-19
static hosts 21-19
IP traceroute
executing 48-12
overview 48-11
IP unicast routing
address resolution 36-7
administrative distances 36-101, 36-110
ARP 36-7
assigning IP addresses to Layer 3 interfaces 36-5
authentication keys 36-111
broadcast
   address 36-14
   flooding 36-15
   packets 36-12
   storms 36-12
classless routing 36-6
configuring static routes 36-100
displaying  39-8
limitations  39-3
matching criteria  39-3
port  39-1
precedence  39-2
router  39-1
supported  39-2
addresses  37-2
address formats  37-2
applications  37-5
assigning address  37-10
autoconfiguration  37-4
CEFv6  37-18
configuring static routes  37-19
default configuration  37-9
default router preference (DRP)  37-4
defined  37-1
Enhanced Interior Gateway Routing Protocol (EIGRP) IPv6  37-6
Router ID  37-6
feature limitations  37-8
features not supported  37-8
forwarding  37-10
ICMP  37-4
monitoring  37-24
neighbor discovery  37-4
OSPF  37-6
path MTU discovery  37-4
SDM templates  6-2, 38-1, 39-1
Stateless Autoconfiguration  37-4
supported features  37-2
switch limitations  37-8
understanding static routes  37-6
IPv6 traffic, filtering  39-3
IRDP
configuring  36-11
definition  36-11
IS-IS
addresses  36-64
area routing  36-64
default configuration  36-65
monitoring  36-73
show commands  36-73
system routing  36-64
ISL
and IPv6  37-3
ISL and trunk ports  9-3
ISO CLNS
clear commands  36-73
dynamic routing protocols  36-64
monitoring  36-73
NETs  36-64
NSAPs  36-64
OSI standard  36-64
ISO IGRP
area routing  36-64
system routing  36-64
isolated port  13-2
isolated VLANs  13-2, 13-3
ITU-T Y.1731
See Y.1731

J

join messages, IGMP  23-3

K

keepalive messages  16-2
Kerberos
authenticating to
boundary switch  7-33
KDC  7-33
network services  7-34
configuration examples  7-31
configuring  7-34
credentials  7-31
cryptographic software image 7-31
described 7-31
KDC 7-31
operation 7-33
realm 7-32
server 7-32
switch as trusted third party 7-31
terms 7-32
TGT 7-33
tickets 7-31
key distribution center
See Kerberos, KDC

L
l2protocol-tunnel command 15-22
L2VPN interworking 44-48
L2VPN pseudowire redundancy 44-46
label binding 44-3
label distribution protocol
See LDP
labels, MPLS 44-2
label switching router
See LSR
LACP
Layer 2 protocol tunneling 15-18
See EtherChannel
Layer 2 frames, classification with CoS 34-2
Layer 2 interfaces, default configuration 9-11
Layer 2 protocol tunneling
bypass mode 15-17, 15-21
configuring 15-19
configuring for EtherChannels 15-23
default configuration 15-20
defined 15-17
guidelines 15-20
Layer 2 traceroute
and ARP 48-10
and CDP 48-10
described 48-10
IP addresses and subnets 48-10
MAC addresses and VLANs 48-10
multicast traffic 48-10
multiple devices on a port 48-11
unicast traffic 48-10
usage guidelines 48-10
Layer 2 trunks 11-15
Layer 3 features 1-10
Layer 3 interfaces
assigning IP addresses to 36-5
assigning IPv4 and IPv6 addresses to 37-13
assigning IPv6 addresses to 37-10
changing from Layer 2 mode 36-5, 36-90
types of 36-3
Layer 3 packets, classification methods 34-3
LDAP 4-2
LDP 44-7
Leaking IGMP Reports 20-4
leave processing, IGMP 23-10
lightweight directory access protocol
See LDAP
line configuration mode 2-2
Link Aggregation Control Protocol
See EtherChannel
See LACP
Link Failure
detecting unidirectional 17-7
link integrity, verifying with REP 19-3
Link Layer Discovery Protocol
See CDP
link local unicast addresses 37-3
link monitoring, Ethernet OAM 43-33, 43-36
link redundancy
See Flex Links
links, unidirectional 27-1
link state advertisements (LSAs) 36-30
link-state tracking
configuring 35-22
Index

Catalyst 3750 Metro Switch Software Configuration Guide

L

LLDP
configuring 26-3
characteristics 26-4
default configuration 26-3
disabling and enabling
globally 26-5
on an interface 26-5
monitoring and maintaining 26-7
overview 26-1
supported TLVs 26-2
switch stack considerations 26-2
transmission timer and holdtime, setting 26-4

LLDP-MED
configuring 26-3
TLVs 26-6
monitoring and maintaining 26-7
overview 26-1, 26-2
supported TLVs 26-2

LLDP Media Endpoint Discovery
See LLDP-MED

LLQ
described 34-40
enabling 34-127
interaction with the egress priority queue 34-127

location TLV 26-3, 26-6
logging messages, ACL 33-9
login authentication
with RADIUS 7-22
with TACACS+ 7-13
login banners 5-17
log messages
See system message logging

Long-Reach Ethernet (LRE) technology 1-15
loop guard
described 18-9
enabling 18-15
low-latency queueing
See LLQ

LSR 44-3

LSP Health Monitor
configuring 44-31
described 44-30

LSP multipath tree trace 44-24

LSP ping
configuring 44-26
described 44-23
over pseudowire
configuring 44-29
described 44-24

LSP traceroute
configuring 44-28
described 44-23

LSP tree trace
defined 44-36
manually configuring 44-36

M

MAC addresses
aging time 5-21
and VLAN association 5-20
building the address table 5-20
default configuration 5-21
disabling learning on a VLAN 5-30
discovering 5-31
displaying 5-30
displaying in the IP source binding table 21-25
dynamic
learning 5-20
removing 5-22
in ACLs 33-27

IP address association 36-7
static
adding 5-27
allowing 5-29, 5-30
characteristics of 5-27
dropping 5-29
removing 5-28
MAC address learning, disabling on a VLAN 5-30
MAC address-table move update
  configuration guidelines 20-8
  configuring 20-12
  default configuration 20-8
  description 20-6
  monitoring 20-14
MAC address-to-VLAN mapping 11-28
MAC extended access lists
  applying to Layer 2 interfaces 33-28
  configuring for QoS 34-66
  creating 33-27
  defined 33-27
  for QoS classification 34-9
macros
  See Smartports macros
Maintenance end points
  See MEPs
Maintenance intermediate points
  See MIPs
manageability features 1-3
management options
  CLI 2-1
  CNS 1-3, 4-1
  SNMP 31-1
manual preemption, REP, configuring 19-14
mapping tables for QoS
  configuring
    CoS-to-DSCP 34-81
    DSCP 34-80
    DSCP-to-CoS 34-84
    DSCP-to-DSCP-mutation 34-85
    IP-precedence-to-DSCP 34-82
    policed-DSCP 34-83
  described 34-17
marking
  action in
    hierarchical policy map 34-111, 34-114
ingress policy map 34-69, 34-79
  described
    hierarchical 34-6, 34-34
    ingress 34-6, 34-14
matching
  IPv6 ACLs 39-3
  matching, ACLs 33-7
maximum aging time
  MStP 17-23
  STP 16-21
maximum hop count, MSTP 17-24
maximum number of allowed devices, port-based authentication 8-17
maximum-paths command 36-51, 36-99
membership mode, VLAN port 11-3
MEPs
  and STP 43-4
  defined 43-3
messages
  logging ACL violations 33-15
  to users through banners 5-17
messages, Ethernet OAM 43-33
metrics, in BGP 36-51
metric translations, between routing protocols 36-106
metro tags 15-2
MIBs
  accessing files with FTP A-4
  location of files A-4
  overview 31-1
  SNMP interaction with 31-5
  supported A-1
MIPs
  and STP 43-4
  defined 43-4
mirroring traffic for analysis 28-1
mismatches, autonegotiation 48-7
module number 9-7
monitoring
  802.1Q tunneling 15-27
  access groups 33-40
ACL configuration 33-40
BGP 36-63
cables for unidirectional links 27-1
CDP 25-4
EIGRP 36-42
E-LMI 43-49
EoMPLS 44-55
Ethernet CFM 43-30, 43-31
Ethernet OAM 43-42
Ethernet OAM protocol 43-42
fallback bridging 47-10
features 1-11
Flex Links 20-14
HSRP 40-10
IGMP
  filters 23-26
  snooping 23-12, 38-11
IP
  address tables 36-16
  multicast routing 45-61
  routes 36-112
IP SLAs operations 41-13
IPv6 37-24
IPv6 ACL configuration 39-8
IS-IS 36-73
ISO CLNS 36-73
Layer 2 protocol tunneling 15-27
MAC address-table move update 20-14
MPLS 44-55
MSDP peers 46-17
multicast router interfaces 23-13, 38-11
multi-VRF CE 36-97
MVR 23-21
network traffic for analysis with probe 28-2
OAM manager 43-49
object tracking 42-13
OSPF 36-34
port
  blocking 24-17
  protection 24-17
private VLANs 13-14
pseudowire redundancy 44-51
REP 19-15
RP mapping information 45-34
SFPs
  status 9-22, 48-8
SFPs status 1-11
source-active messages 46-17
speed and duplex mode 9-14
SSM mapping 45-23
traffic flowing among switches 29-1
traffic suppression 24-17
tunneling 15-27
VLAN
  filters 33-41
  maps 33-41
VLANs 11-14
VMPS 11-32
VTP 12-13
MP-BGP 44-12
MPLS
configuring 44-7
default configuration 44-7
experimental field 44-52
fast link change detection 44-14
fast reroute configuration guidelines 44-15
IP SLAs
  ping 44-30
  trace 44-30
IP SLAs LSP
  ping 44-24
  traceroute 44-24
label 44-2
LSP Health Monitor 44-23, 44-30
LSP ping 44-23
LSP traceroute 44-23
monitoring 44-55
network monitoring 44-24
QoS
  configuring 44-53
  default configuration 44-53
  experimental bits 44-52
  uses 44-51
RSVP hello messages 44-14
TE
  autotunnel, configuring 44-20
  backup autotunnel 44-15
  backup tunnel 44-14, 44-19
  configuration guidelines 44-15
  configuring 44-16
  described 44-13
  fast reroute, configuring 44-18
  fast reroute, described 44-14
  fast reroute failure detection 44-19
  primary autotunnel 44-15
  protected links 44-19
  routing protocol, configuring 44-17
  supported features 44-13
  tunnel, configuring 44-16
  unsupported features 44-14
VPN
  configuration guidelines 44-7
  labels 44-4
  packet flow 44-12
VPN QoS 44-55
MPLS OAM
  configuration guidelines 44-25
  default configuration 44-25
  described 44-21
MPLS Operations, Administration, and Maintenance
  See MPLS OAM
MPLS traffic engineering
  See MPLS TE
mrouter Port 20-3
mrouter port 20-5
MSDP
  benefits of 46-3
clearing MSDP connections and statistics 46-18
  controlling source information
    forwarded by switch 46-11
    originated by switch 46-8
    received by switch 46-13
  default configuration 46-4
dense-mode regions
  sending SA messages to 46-16
  specifying the originating address 46-17
filtering
  incoming SA messages 46-13
  SA messages to a peer 46-12
  SA requests from a peer 46-10
  join latency, defined 46-6
  meshed groups
    configuring 46-15
    defined 46-15
  originating address, changing 46-17
  overview 46-1
  peer-RPF flooding 46-2
  peers
    configuring a default 46-4
    monitoring 46-17
    peering relationship, overview 46-1
    requesting source information from 46-8
  shutting down 46-15
source-active messages
  caching 46-6
  clearing cache entries 46-18
  defined 46-2
  filtering from a peer 46-10
  filtering incoming 46-13
  filtering to a peer 46-12
  limiting data with TTL 46-13
  monitoring 46-17
  restricting advertised sources 46-9
MSTP
  boundary ports
    configuration guidelines 17-15
BPDU filtering
- described 18-3
- enabling 18-12

BPDU guard
- described 18-2
- enabling 18-11

CIST, described 17-3

CIST regional root

CIST root 17-5

configuration guidelines 17-14, 18-10
configuring
- forward-delay time 17-23
- hello time 17-22
- link type for rapid convergence 17-24
- maximum aging time 17-23
- maximum hop count 17-24

CIST
- defined 17-2
- operations within a region 17-3

CST
- defined 17-3
- operations between regions 17-4

default configuration 17-14

default optional feature configuration 18-9

displaying status 17-26
enabling the mode 17-15

EtherChannel guard
- described 18-7
- enabling 18-14

extended system ID
- effects on root switch 17-17
- effects on secondary root switch 17-18
- unexpected behavior 17-17

IEEE 802.1s
implementation 17-6
port role naming change 17-6

instances supported 16-9

interface state, blocking to forwarding 18-2

interoperability and compatibility among modes 16-10

interoperability with 802.1D
- described 17-8
- restarting migration process 17-25

IST
- defined 17-2
- master 17-3
- operations within a region 17-3

loop guard
- described 18-9
- enabling 18-15

mapping VLANs to MST instance 17-16

MST region
- CIST 17-3
- configuring 17-15
- described 17-2
- hop-count mechanism 17-5
- IST 17-2
- supported spanning-tree instances 17-2

overview 17-2

Port Fast
- described 18-2
- enabling 18-10

preventing root switch selection 18-8

root guard
- described 18-8
- enabling 18-15

root switch
- configuring 17-17
- effects of extended system ID 17-17
- unexpected behavior 17-17
- shutdown Port Fast-enabled port 18-2

stack changes, effects of 17-8

status, displaying 17-26
multicast Ethernet loopback (ETH-LB) 43-25
multicast Ethernet loopback, using 43-30
multicast groups
   Immediate Leave 23-5
   joining 23-3
   leaving 23-4
   static joins 23-9, 38-7
multicast packets
   ACLs on 33-40
   blocking 24-8
multicast router interfaces, monitoring 23-13, 38-11
multicast router ports, adding 23-8, 38-8
Multicast Source Discovery Protocol
   See MSDP
multicast storm-control command 24-4
multicast storms 24-1
Multicast VLAN Registration
   See MVR
multioperations scheduling, IP SLAs 41-5
Multiple Spanning Tree Protocol
   See MSTP
multiple VPN routing/forwarding, customer edge devices
   See multi-VRF CE
multiple VPN routing/forwarding in customer edge devices
   See multi-VRF CE
multiprotocol label switching
   See MPLS
multi-VRF CE
   configuration example 36-94
   configuration guidelines 36-86
   configuring 36-85
   default configuration 36-86
   defined 36-83
   displaying 36-97
   monitoring 36-97
   network components 36-85
   packet-forwarding process 36-85
   support for 1-10
MVR
   and address aliasing 23-17
   configuring interfaces 23-18
   default configuration 23-16
   described 23-13
   modes 23-18
   monitoring 23-21
   setting global parameters 23-17
MVRO, guidelines 23-16
MVR over trunk ports
   See MVRO

N
named IP ACLs 33-14
NameSpace Mapper
   See NSM
native VLAN
   and 802.1Q tunneling 15-4
   configuring 11-23
   default 11-23
NEAT
   configuring 8-31
   overview 8-12
neighbor discovery, IPv6 37-4
neighbor discovery/recovery, EIGRP 36-36
neighbor offset numbers, REP 19-4
neighbors, BGP 36-58
Network Edge Access Topology
   See NEAT
network management
   CDP 25-1
   RMON 29-1
   SNMP 31-1
network performance, measuring with IP SLAs 41-3
network policy TLV 26-6
Network Time Protocol
   See NTP
no commands 2-4
nonhierarchical policy maps
34-13
non-IP traffic filtering
33-27
Nonstop Forwarding Awareness
See NSF Awareness
nontrunking mode
11-16
normal-range VLANs
defined
11-1
no switchport command
9-4
not-so-stubby areas
See NSSA
NSAPs, as ISO IGRP addresses
36-64
NSF Awareness
BGP
36-47
EIGRP
36-38
IS-IS
36-66
OSPF
36-26
NSM
4-3
NSSA, OSPF
36-30
NTP
and ACL time ranges
33-16
associations
authenticating
5-4
defined
5-2
enabling broadcast messages
5-6
peer
5-5
server
5-5
default configuration
5-4
displaying the configuration
5-10
overview
5-2
restricting access
creating an access group
5-8
disabling NTP services per interface
5-9
source IP address, configuring
5-10
stratum
5-2
synchronizing devices
5-5
time
services
5-2
synchronizing
5-2
NTP access group keywords, scanning order
5-9
OAM
client
43-32
features
43-33
sublayer
43-32
OAM manager
and E-LMI
43-43
configuration guidelines
43-44
configuring
43-45, 43-51
monitoring
43-49
purpose of
43-43
with CFM
43-43
with CFM and Ethernet OAM
43-50
OAM PDUs
43-34
OAM protocol data units
43-32
object tracking
HSRP
42-7
IP SLAs
42-9
IP SLAs, configuring
42-9
monitoring
42-13
Open Shortest Path First
See OSPF
optimizing system resources
6-1
options, management
1-3
OSPF
area parameters, configuring
36-30
configuring
36-26
default configuration
metrics
36-32
route
36-32
settings
36-25
described
36-23
for IPv6
37-6
interface parameters, configuring
36-27
LSA group pacing
36-33
monitoring
36-34
network types, configuring
36-29
router IDs
36-34
Index

route summarization 36-32
virtual links 36-32

P

packet modification, with QoS 34-55
PAgP
   Layer 2 protocol tunneling 15-18
   See EtherChannel
parallel paths, in routing tables 36-99
passive interfaces
   configuring 36-109
   OSPF 36-32
passwords
   default configuration 7-2
   disabling recovery of 7-5
   encrypting 7-3
   overview 7-1
   recovery of 48-3
   setting
      enable 7-3
      enable secret 7-3
      Telnet 7-6
      with usernames 7-6
   VTP domain 12-7
path cost
   MSTP 17-20
   STP 16-18
path MTU discovery 37-4
PBR
   defined 36-106
   enabling 36-107
   fast-switched policy-based routing 36-108
   local policy-based routing 36-108
peers, BGP 36-58
percentage thresholds in tracked lists 42-6
performance features 1-2
periodic data collection and transfer mechanism 31-6
persistent self-signed certificate 7-41
per-VLAN spanning-tree plus
   See PVST+
PE to CE routing, configuring 36-93
physical ports 9-2
PIM
   default configuration 45-10
   dense mode
      overview 45-4
      rendezvous point (RP), described 45-5
      RPF lookups 45-8
   displaying neighbors 45-62
   enabling a mode 45-12
   overview 45-3
   router-query message interval, modifying 45-37
   shared tree and source tree, overview 45-34
   shortest path tree, delaying the use of sparse mode
      join messages and shared tree 45-5
      overview 45-5
      prune messages 45-5
      RPF lookups 45-8
   stub routing
      configuration guidelines 45-13
      enabling 45-13
      overview 45-5
   versions
      interoperability 45-10
      troubleshooting interoperability problems 45-34
      v2 improvements 45-4
PIM-DVMRP, as snooping method 23-7
ping
   character output description 48-9
   executing 48-8
   overview 48-8
ping, LSP 44-23
ping mpls ipv4 command 44-26
ping mpls pseudowire command 44-29
policed-DSCP map for QoS 34-83
policers
configuring
  for each matched traffic class 34-69
  for more than one traffic class 34-79
  hierarchical, two-rate 34-110
displaying aggregate 34-102
hierarchical, two-rate 34-34
ingress, single-rate 34-14
number supported 34-53, 34-104
types of 34-13
types of ingress 34-13
policies, hierarchical, described 34-34
policing
  hierarchical dual-level on SVIs
    See dual-level policy maps
ingress, described 34-13
token-bucket algorithm 34-14, 34-34
policy-based routing
  See PBR
policy maps
dual-level 34-13
  hierarchical on SVIs 34-13
policy maps for QoS
  characteristics of ingress 34-69
described 34-12, 34-33
displaying 34-102, 34-131
dual-level
  configuring 34-73
described 34-15
  hierarchical on SVIs
    configuring 34-73
described 34-15
nonhierarchical and single-level
  configuring 34-69
described 34-13
port ACLs
  defined 33-2
types of 33-4
Port Aggregation Protocol
  See EtherChannel
port-based authentication
  accounting 8-5
    configuring 8-29
  authentication server
defined 8-2
  RADIUS server 8-2
client, defined 8-2
configuration guidelines 8-16
configuring
guest VLAN 8-26
  host mode 8-25
IEEE 802.1x authentication 8-19
  manual re-authentication of a client 8-22
  periodic re-authentication 8-22
  quiet period 8-22
  RADIUS server 8-21
  RADIUS server parameters on the switch 8-20
  restricted VLAN 8-27
  switch-to-client frame-retransmission number 8-24, 8-25
  switch-to-client retransmission time 8-23
  violation mode 8-7
  violation modes 8-18 to 8-19
default configuration 8-15
described 8-1
device roles 8-2
displaying statistics 8-35
downloadable ACLs and redirect URLs
  configuring 8-33 to 8-35
EAPOL-start frame 8-3
EAP-request/identity frame 8-3
EAP-response/identity frame 8-3
encapsulation 8-3
guest VLAN
  configuration guidelines 8-9, 8-10
described 8-9
  initiation and message exchange 8-3
  maximum number of allowed devices per port 8-17
  method lists 8-19
multiple-hosts mode, described  8-25
per-user ACLs
  AAA authorization  8-19
  configuration tasks  8-11
  described  8-11
  RADIUS server attributes  8-11
ports
  authorization state and dot1x port-control command  8-4
  authorized and unauthorized  8-4
  voice VLAN  8-7
port security
  and voice VLAN  8-7
  described  8-6
  interactions  8-6
  multiple-hosts mode  8-25
readiness check
  configuring  8-17
  described  8-6, 8-17
resetting to default values  8-29
statistics, displaying  8-35
switch
  as proxy  8-3
  RADIUS client  8-3
switch supplicant
  configuring  8-31
  overview  8-12
topologies, supported  8-5
upgrading from a previous release  34-46
user distribution
  guidelines  8-12
  overview  8-12
VLAN assignment
  AAA authorization  8-19
  characteristics  8-8
  configuration tasks  8-8
  described  8-8
voice VLAN
  described  8-7
  PVID  8-7
  VVID  8-7
port blocking  24-7
port-channel
  See EtherChannel
Port Fast
  described  18-2
  enabling  18-10
  mode, spanning tree  11-29
port membership modes, VLAN  11-3
port priority
  MSTP  17-19
  STP  16-16
ports
  access  9-2
  blocking  24-7
  configuring  9-7
  dynamic access  11-3
  enhanced services (ES)  9-3, 9-7
  identifying  9-7
  IEEE 802.1Q tunnel  11-4
  numbering  9-7
  protected  24-6
  REP  19-6
  routed  9-4
  secure  24-8
  static-access  11-3, 11-10
  switch  9-2
  trunks  11-3, 11-15
  VLAN assignments  11-10
port security
  aging  24-15
  and private VLANs  24-16
  and QoS trusted boundary  34-60
  configuration guidelines  24-11
  configuring  24-12
  default configuration  24-11
  described  24-8
  displaying  24-17
Index

enabling 24-16
on trunk ports 24-13
sticky learning 24-9
violations 24-10

port-shutdown response, VMPS 11-28
power management TLV 26-6
preempt delay time, REP 19-5
preemption, default configuration 20-8
preemption delay, default configuration 20-8
preferential treatment of traffic

See QoS
prefix lists, BGP 36-55
preventing unauthorized access 7-1
primary edge port, REP 19-4
primary interface for object tracking, DHCP, configuring 42-10
primary interface for static routing, configuring 42-10
primary links 20-2
primary pseudowire 44-47
primary VLANs 13-1, 13-3

priority
HSRP 40-6
overriding CoS 14-5
trusting CoS 14-5

priority queues for QoS
egress on a standard port 34-25
ingress 34-90
LLQ on an enhanced services port 34-127

private VLAN edge ports
See protected ports

definitions
across multiple switches 13-4
and SDM template 13-4
and SVIs 13-5
benefits of 13-1
community ports 13-2
community VLANs 13-2, 13-3
configuration guidelines 13-7, 13-8
configuration tasks 13-6

configuring 13-10
default configuration 13-6
derending station access to 13-3
IP addressing 13-3
isolated port 13-2
isolated VLANs 13-2, 13-3
mapping 13-13
monitoring 13-14

ports
community 13-2
configuration guidelines 13-8
configuring host ports 13-11
configuring promiscuous ports 13-12

described 11-4
isolated 13-2
promiscuous 13-2
primary VLANs 13-1, 13-3
promiscuous ports 13-2
secondary VLANs 13-2
subdomains 13-1
traffic in 13-5

privileged EXEC mode 2-2

privilege levels
changing the default for lines 7-9
exiting 7-9
logging into 7-9
overview 7-2, 7-7
setting a command with 7-8

promiscuous ports
configuring 13-12
defined 13-2
protected ports 24-6

protocol-dependent modules, EIGRP 36-36

Protocol-Independent Multicast Protocol
See PIM

provider edge devices
and MPLS 44-7
and MPLS labels 44-4
in VPNs 44-6

private VLANs
across multiple switches 13-4
and SDM template 13-4
and SVIs 13-5
benefits of 13-1
community ports 13-2
community VLANs 13-2, 13-3
configuration guidelines 13-7, 13-8
configuration tasks 13-6

configuring 13-10
default configuration 13-6
derending station access to 13-3
IP addressing 13-3
isolated port 13-2
isolated VLANs 13-2, 13-3
mapping 13-13
monitoring 13-14

ports
community 13-2
configuration guidelines 13-8
configuring host ports 13-11
configuring promiscuous ports 13-12

described 11-4
isolated 13-2
promiscuous 13-2
primary VLANs 13-1, 13-3
promiscuous ports 13-2
secondary VLANs 13-2
subdomains 13-1
traffic in 13-5

privileged EXEC mode 2-2

privilege levels
changing the default for lines 7-9
exiting 7-9
logging into 7-9
overview 7-2, 7-7
setting a command with 7-8

promiscuous ports
configuring 13-12
defined 13-2
protected ports 24-6

protocol-dependent modules, EIGRP 36-36

Protocol-Independent Multicast Protocol
See PIM

provider edge devices
and MPLS 44-7
and MPLS labels 44-4
in VPNs 44-6
<table>
<thead>
<tr>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>IN-37</td>
</tr>
<tr>
<td>Catalyst 3750 Metro Switch Software Configuration Guide</td>
</tr>
</tbody>
</table>

| using multi-VRF CE | 36-84 |
| proxy ARP |
| configuring | 36-9 |
| definition | 36-7 |
| with IP routing disabled | 36-10 |
| proxy reports | 20-3 |
| pruning, VTP |
| enabling | 12-12 |
| enabling on a port | 11-22 |
| examples | 12-5 |
| overview | 12-4 |
| pruning-eligible list |
| changing | 11-22 |
| for VTP pruning | 12-4 |
| VLANs | 12-12 |
| pseudowire |
| L2VPN interworking | 44-48 |
| pseudowire class | 44-48 |
| pseudowire redundancy | 44-46 |
| configuration guidelines | 44-47 |
| monitoring | 44-51 |
| pseudowires, defined | 44-46 |
| pseudowire switchover, manually configuring | 44-50 |
| PVST+ |
| described | 16-9 |
| IEEE 802.1Q trunking interoperability | 16-10 |
| instances supported | 16-9 |

| auto-QoS |
| categorizing traffic | 34-41 |
| configuration and defaults display | 34-49 |
| configuration guidelines | 34-45 |
| described | 34-40 |
| disabling | 34-47 |
| effects on running configuration | 34-45 |
| egress queue-set defaults | 34-45 |
| enabling for VoIP | 34-46 |
| example configuration | 34-48 |
| generated commands, displaying | 34-47 |
| ingress queue defaults | 34-41 |
| initial configuration, displaying | 34-49 |
| list of generated commands | 34-43 |
| basic model | 34-4 |
| classification |
| class maps, described | 34-12, 34-33 |
| DSCP transparency, described | 34-61 |
| flowchart, ingress | 34-11 |
| forwarding treatment | 34-3 |
| hierarchical, defined | 34-6 |
| in frames and packets | 34-3 |
| ingress, defined | 34-6 |
| IP ACLs, described | 34-10, 34-11 |
| MAC ACLs, described | 34-9, 34-11 |
| options for IP traffic | 34-10 |
| options for non-IP traffic | 34-9 |
| trust DSCP, described | 34-9 |
| trusted CoS, described | 34-9 |
| trust IP precedence, described | 34-9 |
| class maps |
| configuring hierarchical | 34-108 |
| configuring ingress | 34-67 |
| displaying | 34-102, 34-131 |
| configuration guidelines |
| auto-QoS | 34-45 |
| hierarchical QoS | 34-103 |
| standard QoS | 34-53 |
| configuring | 34-58, 34-104 |
DSCP transparency 34-61
policy maps, dual level 34-73
policy maps, hierarchical on SVIs 34-73

CPU-generated traffic
configuring QoS parameters 34-42
cpu traffic qos command 34-68
default marking 34-54
marking and queuing 34-17, 34-68
mls qos srr-queue output cpu-queue command 34-17, 34-69
queue and threshold values 34-21, 34-25
show cpu traffic qos command 34-50

default configuration
auto-QoS 34-41
hierarchical QoS 34-103
standard QoS 34-50

displaying statistics 34-102
DSCP maps 34-80
DSCP transparency 34-61

egress queue-sets
allocating buffer space 34-91
buffer allocation scheme, described 34-24
characteristics 34-91
configuring shaped weights for SRR 34-95
configuring shared weights for SRR 34-96
described 34-6
displaying the threshold map 34-94
flowchart 34-23
mapping DSCP or CoS values 34-93
priority queuing 34-54, 34-97
scheduling, described 34-6
setting WTD thresholds 34-91
WTD, described 34-25

enabling globally 34-56
flowcharts
egress queue-set queuing and scheduling 34-23
hierarchical queues queuing and scheduling 34-37
hierarchical two-rate policing and marking 34-35

ingress, single-rate policing and marking 34-15
ingress classification 34-11
ingress queuing and scheduling 34-20

hierarchical levels
class level, described 34-30
physical interface level, described 34-32
supported number of class-level classes 34-31
supported number of VLAN-level classes 34-31
VLAN level, described 34-31

hierarchical QoS
CBWFQ 34-39
CBWFQ and DSCP-based WRED 34-119
CBWFQ and IP precedence-based WRED 34-123
CBWFQ and tail drop 34-116
child policy 34-31
classification based on class maps
configuration guidelines 34-103
congestion avoidance 34-38
congestion management 34-38
default class 34-34
default configuration 34-103
displaying 34-131
LLQ 34-40, 34-127
marking 34-34, 34-114
matching criteria 34-33
policing, described 34-34
shaping 34-40, 34-129
tail drop 34-38
traffic policies, described 34-33
two-rate traffic policer 34-34, 34-110
WRED 34-39

See also QoS, hierarchical levels
See also QoS, hierarchical queues

hierarchical queues
average queue size calculation 34-39
bandwidth limited stream 34-30
CBWFQ 34-39
congestion control 34-38
default queue 34-38
described 34-7, 34-38

LLQ 34-40
number of queues supported 34-38
queue creation 34-33
scheduling 34-7
tail drop 34-38
WRED 34-39
See also QoS, hierarchical QoS

implicit deny 34-12

ingress queues
allocating bandwidth 34-89
allocating buffer space 34-88
buffer and bandwidth allocation, described 34-21
characteristics 34-86
configuring shared weights for SRR 34-89
configuring the priority queue described 34-6
displaying the threshold map 34-88
flowchart 34-20
mapping DSCP or CoS values 34-87
priority queue, described 34-22
scheduling, described 34-6
setting WTD thresholds 34-87
WTD, described 34-21
in MPLS networks 44-51

IP phones
automatic classification and queueing 34-41
detection and trusted settings 34-41, 34-60

limiting bandwidth on egress interface 34-97

mapping tables
CoS-to-DSCP 34-81
displaying 34-102
DSCP-to-CoS 34-84
DSCP-to-DSCP-mutation 34-85
IP-precedence-to-DSCP 34-82
policed-DSCP 34-83
types of 34-17

marking
marked-down actions 34-71, 34-76, 34-111, 34-114

MPLS VPN 44-55
overview 34-2

packet modification 34-55

policers
configuring 34-71, 34-76, 34-79
displaying aggregate 34-102
hierarchical, two-rate 34-34
ingress, single-rate 34-14
number supported 34-53, 34-104
types of 34-13
types of ingress 34-13

policies, attaching to an interface 34-14, 34-36

policing
described 34-6
hierarchical, described 34-34
ingress, described 34-13
token-bucket algorithm 34-14

policy maps
characteristics of ingress 34-69
configuring 34-69
described 34-12, 34-33
displaying 34-102, 34-131
dual-level 34-13, 34-15
hierarchical on SVIs 34-13, 34-15

QoS label, defined 34-6
queues
configuring egress queue-set characteristics 34-91
configuring ingress characteristics 34-86
location of 34-17
SRR, described 34-19
WTD, described 34-19
See also QoS, egress queue-sets
See also QoS, hierarchical queues
See also QoS, ingress queues

rewrites 34-55
trusted boundary, configuring 34-60
trust states
- bordering another domain 34-61
- described 34-9
- trusted device 34-60
- within the domain 34-56

VRF 44-55
QoS features 1-8
- See QoS
queries, IGMP 23-3

R

RADIUS
- attributes
  - vendor-proprietary 7-29
  - vendor-specific 7-28
- configuring
  - accounting 7-27
  - authentication 7-22
  - authorization 7-26
  - communication, global 7-20, 7-28
  - communication, per-server 7-19, 7-20
  - multiple UDP ports 7-20
- default configuration 7-19
- defining AAA server groups 7-24
- displaying the configuration 7-30
- identifying the server 7-19
- limiting the services to the user 7-26
- method list, defined 7-19
- operation of 7-18
- overview 7-17
- server load balancing 7-30
- suggested network environments 7-17
- tracking services accessed by user 7-27

range
- macro 9-10
- of interfaces 9-8
- rapid convergence 17-9

rapid per-VLAN spanning-tree plus
- See rapid PVST+
rapid PVST+
- described 16-9
- IEEE 802.1Q trunking interoperability 16-10
- instances supported 16-9
Rapid Spanning Tree Protocol
- See RSTP
RARP 36-7
RCP
- configuration files
  - downloading B-16
  - overview B-14
  - preparing the server B-15
  - uploading B-17
- image files
  - deleting old image B-34
  - downloading B-32
  - preparing the server B-31
  - uploading B-34
- reachability, tracking IP SLAs IP host 42-9
- readiness check
  - port-based authentication
    - configuring 8-17
    - described 8-6, 8-17
- reconfirmation interval, VMPS, changing 11-31
- recovery procedures 48-1
- redirect URL 8-33
- redundancy
  - EtherChannel 35-3
  - HSRP 40-1
  - pseudowire 44-46
  - STP
    - backbone 16-8
    - path cost 11-26
    - port priority 11-24
  - redundant links and UplinkFast 18-13
  - redundant peer 44-50
  - redundant pseudowires 44-47
Index

reliable transport protocol, EIGRP 36-36
reloading software 3-19
Remote Authentication Dial-In User Service
See RADIUS
Remote Copy Protocol
See RCP
remote failure indications 43-33
remote failure indications, Ethernet OAM 43-39
remote loopback, Ethernet OAM 43-33, 43-35
Remote Network Monitoring
See RMON
Remote SPAN
See RSPAN
REP
administrative VLAN 19-9
administrative VLAN, configuring 19-9
age timer 19-8
and STP 19-6
configuration guidelines 19-7
configuring interfaces 19-10
convergence 19-4
default configuration 19-7
manual preemption, configuring 19-14
monitoring 19-15
neighbor offset numbers 19-4
open segment 19-2
ports 19-6
preempt delay time 19-5
primary edge port 19-4
ring segment 19-2
secondary edge port 19-4
segments 19-1
characteristics 19-2
SNMP traps, configuring 19-14
supported interfaces 19-1
triggering VLAN load balancing 19-5
verifying link integrity 19-3
VLAN blocking 19-13
VLAN load balancing 19-4
report suppression, IGMP

described 23-5
disabling 23-12, 38-11
resequencing ACL entries 33-14
reserved addresses in DHCP pools 21-27
resets, in BGP 36-50
resetting a UDLD-shutdown interface 27-6
Resilient Ethernet Protocol (REP)
See REP
responder, IP SLAs

described 41-4
enabling 41-7
response time, measuring with IP SLAs 41-4
restricted VLAN
configuring 8-27

described 8-10
using with IEEE 802.1x 8-10
restricting access
NTP services 5-8
overview 7-1
passwords and privilege levels 7-2
RADIUS 7-16
TACACS+ 7-9
retry count, VMPS, changing 11-32
reverse address resolution 36-7
Reverse Address Resolution Protocol
See RARP
RFC
1058, RIP 36-18
1112, IP multicast and IGMP 23-2
1157, SNMPv1 31-2
1163, BGP 36-43
1166, IP addresses 36-4
1253, OSPF 36-23
1267, BGP 36-43
1305, NTP 5-2
1587, NSSAs 36-23
1757, RMON 29-2
1771, BGP 36-43
1901, SNMPv2C 31-2
1902 to 1907, SNMPv2 31-2
2236, IP multicast and IGMP 23-2
2273-2275, SNMPv3 31-2
RFC4379 44-22

RIP
  advertisements 36-18
  authentication 36-21
  configuring 36-19
  default configuration 36-18
  described 36-18
  for IPv6 37-6
  hop counts 36-18
  split horizon 36-21
  summary addresses 36-21

RMON
  default configuration 29-3
  displaying status 29-6
  enabling alarms and events 29-3
  groups supported 29-2
  overview 29-1
  statistics
    collecting group Ethernet 29-6
    collecting group history 29-5
  root guard
    described 18-8
    enabling 18-15
  root switch
    MSTP 17-17
    STP 16-14
  route calculation timers, OSPF 36-32
  route dampening, BGP 36-62
  routed packets, ACLs on 33-39
  routed ports
    configuring 36-3
    defined 9-4
    IP addresses on 9-18, 36-3
  route-map command 36-108
  route maps
    BGP 36-53
    policy-based routing 36-106
    router ACLs
      defined 33-2
      types of 33-3
    route reflectors, BGP 36-61
    router ID, OSPF 36-34
    route selection, BGP 36-51
    route summarization, OSPF 36-32
    route targets, VPN 36-85
    routing
      dynamic 36-2
      redistribution of information 36-102
      static 36-2
    routing domain confederation, BGP 36-60
  Routing Information Protocol
    See RIP
    routing protocol administrative distances 36-101

RSPAN
  characteristics 28-8
  configuration guidelines 28-16
  default configuration 28-9
  destination ports 28-7
  displaying status 28-23
  interaction with other features 28-8
  monitored ports 28-5
  monitoring ports 28-7
  overview 28-1
  received traffic 28-4
  session limits 28-10
  sessions
    creating 28-16
    defined 28-3
    limiting source traffic to specific VLANs 28-22
    specifying monitored ports 28-16
    with ingress traffic enabled 28-20
    source ports 28-5
    transmitted traffic 28-5
    VLAN-based 28-5
    RSTP
active topology, determining 17-9
BPDU
  format 17-11
  processing 17-12
designated port, defined 17-9
designated switch, defined 17-9
interoperability with 802.1D
  described 17-8
  restarting migration process 17-25
topology changes 17-13
overview 17-8
port roles
  described 17-9
  synchronized 17-11
proposal-agreement handshake process 17-10
rapid convergence
  described 17-9
  edge ports and Port Fast 17-9
  point-to-point links 17-10, 17-24
  root ports 17-10
  root port, defined 17-9
See also MSTP
running configuration
  replacing B-18, B-19
  rolling back B-18, B-19
running configuration, saving 3-15

S
scheduled reals 3-19
scheduling
  egress queue-sets
    priority queueing 34-97
    shaped or shared mode 34-25
    shaped weights 34-95
    shared weights 34-96
    SRR and priority queueing interaction 34-54
    WTD thresholds 34-24, 34-91
  hierarchical queues
CBWFQ 34-39, 34-116
LLQ 34-40, 34-127
  shaping 34-40, 34-129
ingress queues
  priority queueing 34-22, 34-90
  WTD thresholds 34-21, 34-87
scheduling, IP SLAs operations 41-5
SCP
  and SSH 7-47
  configuring 7-47
SDM
  described 6-1
  templates
    configuration guidelines 6-4
    configuring 6-3, 6-4
    number of 6-1
SDM template 39-3
  dual IPv4 and IPv6 6-2
secondary edge port, REP 19-4
secondary VLANs 13-2
Secure Copy Protocol
  See SCP
secure HTTP client
  configuring 7-46
  displaying 7-46
secure HTTP server
  configuring 7-44
  displaying 7-46
secure MAC addresses
  deleting 24-14
  maximum number of 24-10
  types of 24-9
secure ports, configuring 24-8
secure remote connections 7-36
Secure Shell
  See SSH
Secure Socket Layer
  See SSL
security, port 24-8
<table>
<thead>
<tr>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>security features</td>
</tr>
<tr>
<td>sequence numbers in log messages</td>
</tr>
<tr>
<td>server mode, VTP</td>
</tr>
<tr>
<td>service-provider network</td>
</tr>
<tr>
<td>and 802.1Q tunneling</td>
</tr>
<tr>
<td>and customer VLANs</td>
</tr>
<tr>
<td>and EoMPLS</td>
</tr>
<tr>
<td>and MPLS</td>
</tr>
<tr>
<td>configuring MPLS VPNs</td>
</tr>
<tr>
<td>Layer 2 protocols across</td>
</tr>
<tr>
<td>Layer 2 protocol tunneling for EtherChannels</td>
</tr>
<tr>
<td>MSTP and RSTP</td>
</tr>
<tr>
<td>VPNs in</td>
</tr>
<tr>
<td>set-request operation</td>
</tr>
<tr>
<td>severity levels, defining in system messages</td>
</tr>
<tr>
<td>SFPs</td>
</tr>
<tr>
<td>interface numbering</td>
</tr>
<tr>
<td>monitoring status of</td>
</tr>
<tr>
<td>security and identification</td>
</tr>
<tr>
<td>status, displaying</td>
</tr>
<tr>
<td>shaped round robin</td>
</tr>
<tr>
<td>See SRR</td>
</tr>
<tr>
<td>shaping, average-rate</td>
</tr>
<tr>
<td>configuring</td>
</tr>
<tr>
<td>described</td>
</tr>
<tr>
<td>show access-lists hw-summary command</td>
</tr>
<tr>
<td>show and more command output, filtering</td>
</tr>
<tr>
<td>show cdp traffic command</td>
</tr>
<tr>
<td>show configuration command</td>
</tr>
<tr>
<td>show cpu traffic qos</td>
</tr>
<tr>
<td>show forward command</td>
</tr>
<tr>
<td>show interfaces command</td>
</tr>
<tr>
<td>show interfaces switchport</td>
</tr>
<tr>
<td>show l2protocol command</td>
</tr>
<tr>
<td>show lldp traffic command</td>
</tr>
<tr>
<td>show platform forward command</td>
</tr>
<tr>
<td>show running-config command</td>
</tr>
<tr>
<td>displaying ACLs</td>
</tr>
<tr>
<td>interface description in</td>
</tr>
<tr>
<td>shutdown command on interfaces</td>
</tr>
<tr>
<td>shutdown threshold for Layer 2 protocol packets</td>
</tr>
<tr>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>See SNMP</td>
</tr>
<tr>
<td>single session ID</td>
</tr>
<tr>
<td>small-frame arrival rate, configuring</td>
</tr>
<tr>
<td>Smartports macros</td>
</tr>
<tr>
<td>applying Cisco-default macros</td>
</tr>
<tr>
<td>applying global parameter values</td>
</tr>
<tr>
<td>applying macros</td>
</tr>
<tr>
<td>applying parameter values</td>
</tr>
<tr>
<td>configuration guidelines</td>
</tr>
<tr>
<td>creating</td>
</tr>
<tr>
<td>default configuration</td>
</tr>
<tr>
<td>defined</td>
</tr>
<tr>
<td>displaying</td>
</tr>
<tr>
<td>tracing</td>
</tr>
<tr>
<td>SMNP traps, and CFM</td>
</tr>
<tr>
<td>SNAP</td>
</tr>
<tr>
<td>SNMP</td>
</tr>
<tr>
<td>accessing MIB variables with</td>
</tr>
<tr>
<td>agent</td>
</tr>
<tr>
<td>described</td>
</tr>
<tr>
<td>disabling</td>
</tr>
<tr>
<td>and IP SLAs</td>
</tr>
<tr>
<td>authentication level</td>
</tr>
<tr>
<td>community strings</td>
</tr>
<tr>
<td>configuring</td>
</tr>
<tr>
<td>overview</td>
</tr>
<tr>
<td>configuration examples</td>
</tr>
<tr>
<td>configuration guidelines</td>
</tr>
<tr>
<td>default configuration</td>
</tr>
<tr>
<td>engine ID</td>
</tr>
<tr>
<td>groups</td>
</tr>
<tr>
<td>host</td>
</tr>
<tr>
<td>ifIndex values</td>
</tr>
<tr>
<td>informs</td>
</tr>
<tr>
<td>and trap keyword</td>
</tr>
<tr>
<td>described</td>
</tr>
<tr>
<td>Topic</td>
</tr>
<tr>
<td>-------</td>
</tr>
<tr>
<td>differences from traps</td>
</tr>
<tr>
<td>enabling</td>
</tr>
<tr>
<td>limiting access by TFTP servers</td>
</tr>
<tr>
<td>limiting system log messages to NMS</td>
</tr>
<tr>
<td>manager functions</td>
</tr>
<tr>
<td>MIBs</td>
</tr>
<tr>
<td>location of</td>
</tr>
<tr>
<td>supported</td>
</tr>
<tr>
<td>notifications</td>
</tr>
<tr>
<td>overview</td>
</tr>
<tr>
<td>setting CPU threshold notification</td>
</tr>
<tr>
<td>status, displaying</td>
</tr>
<tr>
<td>system contact and location</td>
</tr>
<tr>
<td>trap manager, configuring</td>
</tr>
<tr>
<td>traps</td>
</tr>
<tr>
<td>described</td>
</tr>
<tr>
<td>differences from informs</td>
</tr>
<tr>
<td>enabling</td>
</tr>
<tr>
<td>enabling MAC address notification</td>
</tr>
<tr>
<td>overview</td>
</tr>
<tr>
<td>types of</td>
</tr>
<tr>
<td>users</td>
</tr>
<tr>
<td>versions supported</td>
</tr>
<tr>
<td>SNMP and Syslog Over IPv6</td>
</tr>
<tr>
<td>SNMP traps</td>
</tr>
<tr>
<td>REP</td>
</tr>
<tr>
<td>SNMPv1</td>
</tr>
<tr>
<td>SNMPv2C</td>
</tr>
<tr>
<td>SNMPv3</td>
</tr>
<tr>
<td>snooping, IGMP</td>
</tr>
<tr>
<td>software images</td>
</tr>
<tr>
<td>location in flash memory</td>
</tr>
<tr>
<td>recovery procedures</td>
</tr>
<tr>
<td>scheduling reloads</td>
</tr>
<tr>
<td>tar file format, described</td>
</tr>
<tr>
<td>See also downloading and uploading</td>
</tr>
<tr>
<td>source addresses, in ACLs</td>
</tr>
<tr>
<td>source-and-destination-IP address based forwarding, EtherChannel</td>
</tr>
<tr>
<td>source-and-destination MAC address forwarding, EtherChannel</td>
</tr>
<tr>
<td>source-IP address based forwarding, EtherChannel</td>
</tr>
<tr>
<td>source-MAC address forwarding, EtherChannel</td>
</tr>
<tr>
<td>Source-specific multicast</td>
</tr>
<tr>
<td>SPAN</td>
</tr>
<tr>
<td>configuration guidelines</td>
</tr>
<tr>
<td>default configuration</td>
</tr>
<tr>
<td>destination ports</td>
</tr>
<tr>
<td>displaying status</td>
</tr>
<tr>
<td>interaction with other features</td>
</tr>
<tr>
<td>monitored ports</td>
</tr>
<tr>
<td>monitoring ports</td>
</tr>
<tr>
<td>overview</td>
</tr>
<tr>
<td>received traffic</td>
</tr>
<tr>
<td>session limits</td>
</tr>
<tr>
<td>sessions</td>
</tr>
<tr>
<td>configuring ingress forwarding</td>
</tr>
<tr>
<td>creating</td>
</tr>
<tr>
<td>defined</td>
</tr>
<tr>
<td>limiting source traffic to specific VLANs</td>
</tr>
<tr>
<td>removing destination (monitoring) ports</td>
</tr>
<tr>
<td>specifying monitored ports</td>
</tr>
<tr>
<td>with ingress traffic enabled</td>
</tr>
<tr>
<td>source ports</td>
</tr>
<tr>
<td>transmitted traffic</td>
</tr>
<tr>
<td>VLAN-based</td>
</tr>
<tr>
<td>spanning tree and native VLANs</td>
</tr>
<tr>
<td>Spanning Tree Protocol</td>
</tr>
<tr>
<td>SPAN traffic</td>
</tr>
<tr>
<td>speed, configuring on interfaces</td>
</tr>
<tr>
<td>split horizon</td>
</tr>
<tr>
<td>IGRP</td>
</tr>
<tr>
<td>RIP</td>
</tr>
</tbody>
</table>
SRR
and priority queueing interaction 34-54
configuring
  shaped weights on egress queue-sets 34-95
  shared weights on egress queue-sets 34-96
  shared weights on ingress queues 34-89
described 34-19
shaped mode 34-19
shared mode 34-20

SSH
configuring 7-37
cryptographic software image 7-36
described 7-36
encryption methods 7-37
user authentication methods, supported 7-37

SSL
configuration guidelines 7-43
configuring a secure HTTP client 7-46
configuring a secure HTTP server 7-44
cryptographic software image 7-40
described 7-40
monitoring 7-46

SSM
address management restrictions 45-16
CGMP limitations 45-17
components 45-15
configuration guidelines 45-16
configuring 45-14, 45-17
differs from Internet standard multicast 45-15
IGMP snooping 45-17
IGMPv3 45-15
IGMPv3 Host Signalling 45-16
IP address range 45-15
monitoring 45-17
operations 45-15
PIM 45-15
state maintenance limitations 45-17
SSM mapping 45-18
configuration guidelines 45-18
configuring 45-18, 45-20
DNS-based 45-19, 45-21
monitoring 45-23
overview 45-18
restrictions 45-18
static 45-19, 45-21
static traffic forwarding 45-22
stack changes, effects on, MSTP 17-8
standby ip command 40-5
standby links 20-2
standby router 40-1
standby timers, HSRP 40-9
startup configuration
  booting
    manually 3-17
    specific image 3-17
clearing B-18
configuration file
  automatically downloading 3-16
  specifying the filename 3-16
default boot configuration 3-15
static access ports
  assigning to VLAN 11-10
defined 9-3, 11-3
static addresses
  See addresses
static route primary interface, configuring 42-10
static routes
  configuring for IPv6 37-19
  understanding 37-6
static routes, configuring 36-100
static routing 36-2
static routing support, enhanced object tracking 42-10
static SSM mapping 45-19, 45-21
static traffic forwarding 45-22
static VLAN membership 11-2
statistics
  CDP 25-4
  IEEE 802.1x 8-35
interface 9-22
IP multicast routing 45-62
LLDP 26-7
LLDP-MED 26-7
OSPF 36-34
QoS ingress and egress 34-102
RMON group Ethernet 29-6
RMON group history 29-5
SNMP input and output 31-24
VTP 12-13

sticky secure MAC address learning 24-9
storm control
configuring 24-3
described 24-1
disabling 24-5
displaying 24-17

STP
accelerating root port selection 18-4
and REP 19-6
BackboneFast
described 18-5
enabling 18-13
BPDU filtering
described 18-3
enabling 18-12
BPDU guard
described 18-2
enabling 18-11
BPDU message exchange 16-3
configuration guidelines 16-12, 18-10
configuring
forward-delay time 16-21
hello time 16-20
maximum aging time 16-21
path cost 16-18
port priority 16-16
root switch 16-14
secondary root switch 16-16
spanning-tree mode 16-13
switch priority 16-19
counters, clearing 16-22
default configuration 16-11
default optional feature configuration 18-9
designated port, defined 16-3
designated switch, defined 16-3
detecting indirect link failures 18-5
disabling 16-14
displaying status 16-22
EtherChannel guard
described 18-7
disabling 18-14
enabling 18-14
extended system ID
effects on root switch 16-14
effects on the secondary root switch 16-16
overview 16-4
unexpected behavior 16-15
IEEE 802.1D and bridge ID 16-4
IEEE 802.1D and multicast addresses 16-8
IEEE 802.1t and VLAN identifier 16-4
inferior BPDU 16-3
instances supported 16-9
interface state, blocking to forwarding 18-2
interface states
blocking 16-5
disabled 16-7
forwarding 16-5, 16-6
learning 16-6
listening 16-6
overview 16-4
interoperability and compatibility among modes 16-10
keepalive messages 16-2
Layer 2 protocol tunneling 15-17
limitations with IEEE 802.1Q trunks 16-10
load sharing
overview 11-23
using path costs 11-26
using port priorities  11-24
loop guard
described  18-9
enabling  18-15
modes supported  16-9
multicast addresses, effect of  16-8
overview  16-2
path costs  11-26
Port Fast
described  18-2
enabling  18-10
port priorities  11-24
preventing root switch selection  18-8
protocols supported  16-9
redundant connectivity  16-8
root guard
described  18-8
enabling  18-15
root port, defined  16-3
root switch
configuring  16-14
effects of extended system ID  16-4, 16-14
election  16-3
unexpected behavior  16-15
shutdown Port Fast-enabled port  18-2
status, displaying  16-22
superior BPDU  16-3
timers, described  16-20
UplinkFast
described  18-3
enabling  18-13
VLAN-bridge  16-10
stratum, NTP  5-2
stub areas, OSPF  36-30
stub routing, EIGRP  36-41
subdomains, private VLAN  13-1
subnet mask  36-5
subnet zero  36-5
success response, VMPS  11-28
summer time  5-13
SunNet Manager  1-3
supernet  36-6
SVI  34-73
SVIs
and IP unicast routing  36-3
and router ACLs  33-3
connecting VLANs  9-6
defined  9-4
routing between VLANs  11-2
switch  37-2
switch console port  1-4
Switch Database Management
   See SDM
switched packets, ACLs on  33-38
Switched Port Analyzer
   See SPAN
switched ports  9-2
switchport backup interface  20-4, 20-5
switchport block multicast command  24-8
switchport block unicast command  24-8
switchport command  9-11
switchport mode dot1q-tunnel command  15-7
switchport protected command  24-7
switch priority
  MSTP  17-21
  STP  16-19
switch software features  1-1
switch virtual interface
   See SVI
synchronization, BGP  36-47
syslog
   See system message logging
system clock
   configuring
daylight saving time  5-13
manually  5-11
summer time  5-13
time zones  5-12
displaying the time and date 5-11
overview 5-1
See also NTP

system message logging
default configuration 30-3
defining error message severity levels 30-8
disabling 30-4
displaying the configuration 30-13
enabling 30-4
facility keywords, described 30-13
level keywords, described 30-9
limiting messages 30-9
message format 30-2
overview 30-1
sequence numbers, enabling and disabling 30-7
setting the display destination device 30-4
synchronizing log messages 30-5
timestamps, enabling and disabling 30-7
UNIX syslog servers
  configuring the daemon 30-11
  configuring the logging facility 30-12
  facilities supported 30-13

system MTU
  and EoMPLS 44-42
  and IEEE 802.1Q tunneling 15-5
  and IS-IS LSPs 36-68
  configuring 9-19
  maximum size supported 9-19

system name
  default configuration 5-15
  default setting 5-15
  manual configuration 5-15
See also DNS

system prompt, default setting 5-14, 5-15

system resources, optimizing 6-1

system routing
  IS-IS 36-64
  ISO IGRP 36-64

System-to-Intermediate System Protocol

See IS-IS

TACACS+
accounting, defined 7-11
authentication, defined 7-11
authorization, defined 7-11
configuring
  accounting 7-16
  authentication key 7-12
  authorization 7-15
  login authentication 7-13
default configuration 7-12
displaying the configuration 7-16
identifying the server 7-12
limiting the services to the user 7-15
operation of 7-11
overview 7-10
tracking services accessed by user 7-16

tag distribution protocol
  See TDP
tagged packets
  IEEE 802.1Q 15-3
  Layer 2 protocol 15-17
tail drop
  configuring 34-116
described 34-38
tar files
  creating B-5
displaying the contents of B-6
  extracting B-7
  image file format B-23
TCL script, registering and defining with embedded event manager 32-7
TDP 44-7

Telnet
  accessing management interfaces 2-9
  number of connections 1-4
Index

setting a password 7-6

templates, Ethernet OAM 43-39
templates, SDM 6-1
temporary self-signed certificate 7-41
Terminal Access Controller Access Control System Plus
  See TACACS+
terminal lines, setting a password 7-6
TFTP
  configuration files
    downloading B-10
    preparing the server B-10
    uploading B-11
  configuration files in base directory 3-7
  configuring for autoconfiguration 3-7
image files
  deleting B-26
  downloading B-25
  preparing the server B-24
  uploading B-26
  limiting access by servers 31-18
threshold, traffic level 24-2
threshold monitoring, IP SLAs 41-6
time
  See NTP and system clock
time-range command 33-16
time ranges in ACLs 33-16
timestamps in log messages 30-7
time zones 5-12
TLVs
  defined 26-2
  LLDP 26-2
  LLDP-MED 26-2
Token Ring VLANs
  support for 11-6
  VTP support 12-4
traceroute, Layer 2
  and ARP 48-10
  and CDP 48-10
  described 48-10
  IP addresses and subnets 48-10
  MAC addresses and VLANs 48-10
  multicast traffic 48-10
  multiple devices on a port 48-11
  unicast traffic 48-10
  usage guidelines 48-10
traceroute, LSP 44-23
traceroute command 48-12
  See also IP traceroute
traceroute mpls ipv4 command 44-28, 44-36
tracked lists
  configuring 42-3
  types 42-3
tracked objects
  by Boolean expression 42-4
  by threshold percentage 42-6
  by threshold weight 42-5
  tracking interface line-protocol state 42-2
  tracking IP routing state 42-2
  tracking objects 42-1
  tracking process 42-1
  track state, tracking IP SLAs 42-9
traffic
  blocking flooded 24-8
  fragmented 33-5
  fragmented IPv6 39-2
  unfragmented 33-5
traffic shaping
  See shaping, average-rate
transparent mode, VTP 12-3, 12-10
trap-door mechanism 3-2
traps
  configuring MAC address notification 5-22, 5-24, 5-26
  configuring managers 31-12
  defined 31-4
  enabling 5-22, 5-24, 5-26, 31-12
  notification types 31-14
  overview 31-1, 31-5
  troubleshooting
Index

connectivity problems 48-8, 48-9, 48-11
CPU utilization 48-17
detecting unidirectional links 27-1
determining packet forwarding 48-14
displaying crash information 48-17
PIMv1 and PIMv2 interoperability problems 45-34
SFP security and identification 48-7
show forward command 48-14
with CiscoWorks 31-5
with debug commands 48-13
with ping 48-8
with system message logging 30-1
with traceroute 48-11
trunk failover
See link-state tracking
trunk ports
and Layer 2 protocol tunneling 15-20
configuring 11-20
defined 9-3, 11-3
encapsulation 11-20, 11-25, 11-26
secure MAC addresses on 24-12
trunks
allowed-VLAN list 11-21
configuring 11-20, 11-25, 11-26
load sharing
setting STP path costs 11-26
using STP port priorities 11-24
native VLAN for untagged traffic 11-23
parallel 11-26
pruning-eligible list 11-22
to non-DTP device 11-15
understanding 11-15
trusted boundary for QoS 34-60
trusted port states
between QoS domains 34-61
classification options 34-9
ensuring port security for IP phones 34-60
within a QoS domain 34-56
trustpoints, CA 7-41
tunneling
defined 15-1
IEEE 802.1Q 15-2
Layer 2 protocol 15-17
tunnel ports
defined 11-4
described 9-4, 15-2
IEEE 802.1Q, configuring 15-6
incompatibilities with other features 15-6
twisted-pair Ethernet, detecting unidirectional links 27-1
type of service 1-8

U

UDLD
aggressive mode, described 27-1
and autonegotiation 27-1
configuration guidelines 27-4
default configuration 27-4
echoing detection mechanism 27-3
enabling
  globally 27-5
  per interface 27-5
Layer 2 protocol tunneling 15-19
link-detection mechanism 27-1
modes of operation 27-1
neighbor database 27-2
normal mode, described 27-1
overview 27-1
resetting an interface 27-6
status, displaying 27-6
unidirectional link, defined 27-2
UDP, configuring 36-14
UDP jitter, configuring 41-9
UDP jitter operation, IP SLAs 41-8
unauthorized ports with IEEE 802.1x 8-4
unicast MAC address filtering 1-3
  and adding static addresses 5-28
  and broadcast MAC addresses 5-28
and CPU packets  5-28
and multicast addresses  5-28
and router MAC addresses  5-28
configuration guidelines  5-28
described  5-28
unicast storm control command  24-4
unicast storms  24-1
unicast traffic, blocking  24-8
UniDirectional Link Detection protocol
    See UDLD
UNIs, remote (CFM)  43-43
UNIX syslog servers
    daemon configuration  30-11
    facilities supported  30-13
    message logging configuration  30-12
unrecognized Type-Length-Value (TLV) support  12-4
upgrading software images
    See downloading
upgrading with CNS  4-14
UplinkFast
    described  18-3
    enabling  18-13
uploading
    configuration files
        preparing  B-10, B-12, B-15
        reasons for  B-8
        using FTP  B-13
        using RCP  B-17
        using TFTP  B-11
    image files
        preparing  B-24, B-27, B-31
        reasons for  B-22
        using FTP  B-30
        using RCP  B-34
        using TFTP  B-26
User Datagram Protocol
    See UDP
user EXEC mode  2-2
username-based authentication  7-6

V
VCs  44-40
version-dependent transparent mode  12-4
virtual connections
    See VCs
virtual private LAN service
    See VPLS
Virtual Private Networks
    See VPNs
virtual router  40-1, 40-2
vlan.dat file  11-5
VLAN 1, disabling on a trunk port  11-21
VLAN 1 minimization  11-21
VLAN ACLs
    See VLAN maps
vlan-assignment response, VMPS  11-28
VLAN blocking, REP  19-13
VLAN configuration
    at bootup  11-7
    saving  11-7
VLAN configuration mode  2-2
VLAN database
    and startup configuration file  11-7
    and VTP  12-1
    VLAN configuration saved in  11-7
    VLANs saved in  11-4
VLAN filtering, and SPAN  28-6
vlan global configuration command  11-6
VLAN ID
    customer-side  15-7
    discovering  5-31
    mapping  15-7
    service provider  15-8
VLAN IDs, number supported  1-6
VLAN ID translation
    See VLAN mapping
VLAN load balancing
    REP  19-4
INDEX

VLAN load balancing, triggering 19-5
VLAN load balancing on flex links 20-2
configuration guidelines 20-8
VLAN management domain 12-2
VLAN Management Policy Server
See VMPS
VLAN map entries, order of 33-30
VLAN mapping
  802.1Q traffic 15-10
  configuring 15-9
  described 15-7
VLAN maps
  applying 33-34
  common uses for 33-34
  configuration example 33-35
  configuration guidelines 33-30
  configuring 33-29
  creating 33-31
  defined 33-2
  denying access example 33-36
  denying and permitting packets 33-31
  displaying 33-41
  examples 33-35
  with router ACLs 33-40
VLAN membership
  confirming 11-31
  modes 11-3
VLAN Query Protocol
See VQP
VLANs
  adding to VLAN database 11-8
  aging dynamic addresses 16-9
  allowed on trunk 11-21
  and spanning-tree instances 11-3, 11-6, 11-12
  configuration guidelines
    extended-range VLANs 11-11
    normal-range VLANs 11-6
  configuring 11-1
  configuring IDs 1006 to 4094 11-11
  connecting through SVIs 9-6
  creating 11-8
  customer numbering in service-provider networks 15-3
  default configuration 11-7
  deleting 11-9
  described 9-2, 11-1
  displaying 11-14
  extended-range 11-1, 11-11
  features 1-6
  illustrated 11-2
  internal 11-12
  limiting source traffic
    with RSPAN 28-22
    with SPAN 28-14
  modifying 11-8
  native, configuring 11-23
  normal-range 11-1, 11-4
  number supported 1-6
  parameters 11-5
  port membership modes 11-3
  static-access ports 11-10
  STP and IEEE 802.1Q trunks 16-10
  supported 11-2
  Token Ring 11-6
  traffic between 11-2
  VLAN-bridge STP 16-10, 47-1
  VTP modes 12-3
VLAN Trunking Protocol
See VTP
VLAN trunks 11-15
VMPS
administrating 11-32
configuration example 11-33
configuration guidelines 11-29
default configuration 11-29
description 11-27
dynamic port membership
  described 11-28
reconfirming 11-31
troubleshooting 11-33
entering server address 11-30
mapping MAC addresses to VLANs 11-28
monitoring 11-32
reconfirmation interval, changing 11-31
reconfirming membership 11-31
retry count, changing 11-32
voice-over-IP 14-1
voice VLAN
Cisco 7960 phone, port connections 14-1
configuration guidelines 14-3
configuring IP phones for data traffic
  override CoS of incoming frame 14-5
  trust CoS priority of incoming frame 14-5
configuring ports for voice traffic in
  802.1P priority tagged frames 14-5
  802.1Q frames 14-4
connecting to an IP phone 14-4
default configuration 14-3
described 14-1
displaying 14-6
VPN routing and forwarding table
  See VRF
VPNs
  and multi-VRF CE 36-92
  benefits 44-4
  configuring 44-8
  configuring routing sessions 36-92
  described 44-3
  forwarding in 36-86
  in service provider networks 36-83
IPv4 prefix 44-6
MPLS 44-6
number supported 44-7
routes 36-84, 44-3, 44-6
VQP 11-27
VRF
  configuration 44-8
  defining 36-85
  elements 44-3
  in MPLS VPNs 44-3
  tables 36-83
VRF-aware services
  ARP 36-89
  configuring 36-88
  ftp 36-91
  HSRP 36-90
  ping 36-89
  RADIUS 36-91
  SNMP 36-89
  syslog 36-90
  tftp 36-91
  traceroute 36-91
VRF QoS 44-55
VRFs
  configuring multicast 36-92
VTP
  adding a client to a domain 12-12
  advertisements 11-19, 12-3
  and extended-range VLANs 12-1
  and normal-range VLANs 12-2
  client mode, configuring 12-9
  configuration
    guidelines 12-6
    requirements 12-8
    saving 12-7
  configuration requirements 12-8
  configuration revision number
    guideline 12-12
    resetting 12-13
  configuring
    client mode 12-9
    server mode 12-8
    transparent mode 12-10
consistency checks 12-4
default configuration 12-6
described 12-1
disabling 12-10
domain names 12-7
domains 12-2
Layer 2 protocol tunneling 15-17
modes
  client 12-3, 12-9
  server 12-3, 12-8
  transitions 12-3
  transparent 12-3, 12-10
monitoring 12-13
passwords 12-7
pruning
  disabling 12-12
  enabling 12-12
  examples 12-5
  overview 12-4
pruning-eligible list, changing 11-22
server mode, configuring 12-8
statistics 12-13
Token Ring support 12-4
transparent mode, configuring 12-10
using 12-1
version, guidelines 12-8
version 1 12-4
version 2
  configuration guidelines 12-8
  disabling 12-11
  enabling 12-11
  overview 12-4

W

Weighted Random Early Detection
See WRED
weighted tail drop
See WTD

weight thresholds in tracked lists 42-5
WRED
  configuring DSCP-based 34-119
  configuring IP precedence-based 34-123
described 34-39
WTD
described 34-19
setting thresholds
  egress queue-sets 34-91
  ingress queues 34-87

X

xconnect command 44-49
XMODEM protocol 48-2

Y

Y.1731
default configuration 43-25
described 43-23
ETH-AIS
  Ethernet Alarm Signal function (ETH-AIS) 43-24
  ETH-LCK 43-25
  configuring 43-27
  ETH-RDI 43-24
  multicast Ethernet loopback 43-30
  multicast ETH-LB 43-25
terminology 43-23